USER'S GUIDE

KASPERSKY INTERNET SECURITY 2009

Dear User of Kaspersky Internet Security 2009!

Thank you for choosing our product. We hope that this documentation will help you in your work and will provide answers regarding this software product.

Warning! This document is a property of Kaspersky Lab's and all rights to this document are reserved by the copyright laws of the Russian Federation and international treaties. Illegal reproduction and distribution of this document or parts thereof result in civil, administrative or criminal liability pursuant to the laws of the Russian Federation. Any type of reproduction and distribution of any materials, including their translation, is allowed only by a written permission of Kaspersky Lab. This document and graphic images related to it can be used exclusively for information, non-commercial or personal purposes.

This document can be amended with no prior notification. For the latest version of this document refer to Kaspersky Lab's website at http://www.kaspersky.com/docs. Kaspersky Lab does not assume any liability for the content, quality, relevancy or accuracy of the materials used in this document rights for which are held by third parties and for the potential damages associated with using such documents.

This document includes registered and non-registered trademarks. All said trademarks are the property of their corresponding owners.

© Kaspersky Lab, 1996-2008

+7 (495) 645-7939,
Tel., fax: +7 (495) 797-8700,
+7 (495) 956-7000

http://www.kaspersky.com/
http://support.kaspersky.com/

Revision date: April 29, 2008

TABLE OF CONTENT

INTRODUCTION 6
Obtaining information about the application 6
Sources of information to research on your own 6
Contacting the Sales Department 7
Contacting the Technical Support service 7
Discussing Kaspersky Lab applications on the web forum 9
What's new in Kaspersky Internet Security 2009 9
Application protection concept 11
Wizards and Tools 12
Support features 13
Heuristic analysis 13
Hardware and software system requirements 15
THREATS TO COMPUTER SECURITY 16
Threat applications 16
Malicious programs 17
Viruses and worms 17
Trojans 20
Malicious utilities 26
Potentialy unwanted programs 29
Adware 30
Pornware 30
Other Riskware Programs 31
Methods of detecting infected, suspicious and potentially dangerous objects by the application 35
Internet threats 35
Spam or unsolicited incoming mail 36
Phishing 36
Hacker attacks 37
Banners display 37
INSTALLING APPLICATION ON THE COMPUTER 39
Step 1. Searching for a newer version of the application 40

Step 2. Verifying the system's conformity to the installation requirements ... 41
Step 3. Wizard's greeting window ... 41
Step 4. Viewing the License Agreement ... 41
Step 5. Selecting the installation type ... 42
Step 6. Selecting the installation folder ... 42
Step 7. Selecting application components to be installed ... 43
Step 8. Searching for other anti-virus software ... 44
Step 9. Final preparation for the installation ... 45
Step 10. Completing the installation ... 45

APPLICATION INTERFACE ... 46
Notification area icon ... 46
Shortcut menu ... 47
Main application window ... 49
Notifications ... 52
Application settings configuration window ... 52

GETTING STARTED ... 54
Selecting network type ... 55
Updating the application ... 56
Security analysis ... 56
Scanning computer for viruses ... 57
Participating in Kaspersky Security Network ... 58
Security management ... 59
Pausing protection ... 61

VALIDATING APPLICATION SETTINGS ... 63
Test "virus" EICAR and its modifications ... 63
Testing the HTTP traffic protection ... 67
Testing the SMTP traffic protection ... 67
Validating File Anti-Virus settings ... 68
Validating virus scan task settings ... 69
Validating Anti-Spam settings ... 69

KASPERSKY SECURITY NETWORK DATA COLLECTION STATEMENT ... 70

KASPERSKY LAB ... 76
Other Kaspersky Lab Products ... 77

Contact Us 86
CRYPTOEX LLC 88
MOZILLA FOUNDATION 89
LICENSE AGREEMENT 90

INTRODUCTION

IN THIS SECTION:

Obtaining information about the application 6

What's new in Kaspersky Internet Security 2009 9

Application protection concept 11

Hardware and software system requirements 14

OBTAINING INFORMATION ABOUT THE APPLICATION

If you have any questions regarding purchasing, installing or using the application, you can easily receive answers to them.

Kaspersky Lab has many sources of information and you can select the source most convenient to you depending on how urgent and important your question is.

SOURCES OF INFORMATION TO RESEARCH ON YOUR OWN

You can use the **Help** system.

Help system contains information on managing the computer protection: view the protection status, scan various areas of the computer and perform other tasks.

To open Help, click the **Help** link in the main application window or press **<F1>**.

CONTACTING THE SALES DEPARTMENT

If you have questions regarding selecting or purchasing the application or extending the period of its use, you can phone Sales Department specialists in our Central Office in Moscow at:

+7 (495) 797-87-00, **+7 (495) 645-79-39**, **+7 (495) 956-70-00**.

The service is provided in Russian or English.

You can send your questions to the Sales Department to e-mail address sales@kaspersky.com.

CONTACTING THE TECHNICAL SUPPORT SERVICE

If you already purchased the application you can obtain information about it from the Technical Support service by phone or via internet.

The Technical Support service specialists will answer your questions regarding the installation and the use of the application and if your computer has been infected, will help you eliminate the consequences of the activities of malware.

Before contacting the Technical Support service please read the support rules (http://support.kaspersky.com/support/rules).

An e-mail request to the Technical Support service (for registered users only)

You can ask your question to the Technical Support Service specialists by filling out a Helpdesk web form (http://support.kaspersky.com/helpdesk.html).

You can send your question in Russian, English, German, French or Spanish.

In order to send an e-mail message with your question, you must indicate the **client number** obtained during the registration at the Technical Support service website along with your **password**.

Note

If you are not yet a registered user of Kaspersky Lab's applications, you can fill out a registration form (https://support.kaspersky.com/en/PersonalCabinet/Registration/Form/). During the registration you will have to supply the activation code or key file name.

You will receive a Technical Support service specialist's response to your request in your **Personal Cabinet** (https://support.kaspersky.com/en/PersonalCabinet) and at the e-mail address you have specified in your request.

Describe the problem you have encountered in the request web form with as much detail as possible. Specify the following in the mandatory fields:

- **Prompt type**. Questions most frequently asked by users are grouped into special topics, for example "Product installation/removal problem" or "Virus scan/removal problem". If you have not found an appropriate topic, select "General Question".
- **Application name and version number**.
- **Prompt text**. Describe the problem you have encountered with as much detail as possible.
- **Client number and password**. Enter the client number and the password which you have received during the registration at Technical Support service website.
- **E-mail address**. The Technical Support service specialists will use this e-mail address to send their answer to your question.

Technical support by phone

If you have a problem requiring urgent help, you can call the Technical Support service located in your town. Please do not forget to supply necessary information (http://support.kaspersky.com/support/details) when you apply to Russian (http://support.kaspersky.com/support/support_local) or international (http://support.kaspersky.com/support/international) Technical Support. This will help our specialists to process you request as soon as possible.

DISCUSSING KASPERSKY LAB APPLICATIONS ON THE WEB FORUM

If your question does not require an urgent answer, you can discuss it with Kaspersky Lab's specialists and other users of Kaspersky Lab's anti-virus applications in our forum located at Kaspersky Lab's web forum http://forum.kaspersky.com.

In this forum you can view topics published earlier, leave your comments, create new topics and use the search engine.

WHAT'S NEW IN KASPERSKY INTERNET SECURITY 2009

Kaspersky Internet Security 2009 is a totally new approach to data security. The main feature of the application is restricting the programs' rights to access the system resources. It helps prevent unwanted actions by suspicious and hazardous programs. The application's capabilities in the protection of user's confidential data have been considerably enhanced. The application now includes wizards and tools which substantially facilitate execution of specific computer protection tasks.

Let's take closer look at the new features in Kaspersky Internet Security 2009:

New Protection Features

- Kaspersky Internet Security now includes Application Filtering component along with Proactive Defense and Firewall which implements a new universal approach to the system protection against any threats including existing threats and threats that are unknown at the moment. Kaspersky Internet Security now requires considerably less input from the user due to the use of lists of trusted applications (whitelisting).

- Scanning of operating system and software for vulnerabilities with their subsequent elimination maintains a high system security level and prevents sneaking of hazardous programs into your system.

- New wizards – Security Analyzer and Browser Configuration facilitate the scanning for and elimination of security threats and vulnerabilities in

the applications installed on your computer, operating system's and browser settings.

- Kaspersky Lab now reacts to new threats faster due to the use of Participating in Kaspersky Security Network technology that gathers data about infection of users' computers and sends it to Kaspersky Lab's servers.
- New tools – Network Monitor and Network Package Analysis - facilitate collection and analysis of information about network activities on your computer.
- New wizard – System Restore helps fix system damages after malware attacks.

New confidential data protection features:

- A new component Application Filtering effectively monitors access to confidential data, user's file and folders by applications.
- Security of confidential data entered from the keyboard is ensured by a new tool – Virtual keyboard.
- Kaspersky Internet Security structure includes Privacy Cleaner wizard which deletes all information about his or her actions which can present an interest to intruders (list of visited websites, opened files, cookies, etc.) from the user's computer.

New anti-spam features:

- Efficiency of spam filtering by the Anti-Spam component has been increased due to the use of Recent Terms server technologies.
- The use of Microsoft Office Outlook, Microsoft Outlook Express, The Bat! and Thunderbird extension plug-ins simplifies the process of configuring the anti-spam settings.
- Revised Parental Control component allows effective restriction of undesirable access of some internet resources by children.

New protection features for internet use:

- Protection against internet intruders has been upgraded due to the extended databases of phishing sites.
- ICQ and MSN traffic scan has been added which ensures safety of the use of internet pagers.
- Security of the use of wireless networks is ensured through the scan of Wi-Fi connections.

New program's interface features

- The new program's interface reflects the comprehensive approach to information protection.
- High information capacity of dialog boxes helps user quickly make decisions.
- The functionality of reports and statistics information about the application's operation has been extended. The possibility of using filters allowing flexible setup when working with reports makes this product irreplaceable for professionals.

APPLICATION PROTECTION CONCEPT

Kaspersky Internet Security ensures protection of your computer against known and new threats, hacker and intruder attacks, spam and other unwanted data. Each type of threats is processed by an individual application's component. This makes setup flexible, with easy configuration options for all of the components tailored to the needs of a specific user or business as a whole.

Kaspersky Internet Security includes:

- Application's activities monitoring in the system preventing execution of dangerous actions by applications.
- Malware protection components, providing real-time protection of all data transfer and input paths through your computer.
- Components of protection when working in the internet ensuring protection of your computer against network and intruder attacks known at the moment.
- Components of filtering of unwanted data helping save time, web traffic and money.
- Virus scan tasks, used to scan individual files, folders, drives, or areas for viruses or to perform a full computer scan. Scan tasks can be configured to detect vulnerabilities in the applications installed on the computer.
- Update, providing internal application modules state, and also are used for threats scan, hack attacks and spam messages detection.
- Wizards and tools facilitating execution of tasks occurring during the operation of Kaspersky Internet Security.

- Support features which provide information support for working with the application and expanding its capabilities.

WIZARDS AND TOOLS

Ensuring computer security is a rather difficult task requiring knowledge about operating system's features and methods utilized to take advantage of its weaknesses. Besides, a large number and diversity of information about the system security makes it analysis and processing more difficult.

In order to make specific computer security tasks easier to perform Kaspersky Internet Security includes a number of wizards and tools:

- Security Analyzer Wizard that performs computer diagnostics and searches for vulnerabilities in the operating system and programs installed on the computer.
- Browser Configuration Wizard that performs analysis of Microsoft Internet Explorer browser settings evaluation them, first of all, from the security point of view.
- System Restore Wizard is used to eliminate the traces of the malware objects presence in the system.
- Privacy Cleaner Wizard that searches for and eliminates traces of user's activities in the system and operating system's settings which allow gathering of information about the user's activities.
- The Resque Disk is designed to restore system functionality after a virus attack that damaged system files of the operating system and made it impossible to startup.
- Network Package Analysis that intercepts network packets and displays their details.
- Network Monitor that displays details about the network activity on your computer.
- Virtual keyboard allows to prevent interception of data entered from the keyboard.

SUPPORT FEATURES

The application includes a number of support features. They are designed to provide maintain the application up-to-date, expand the capabilities of the program and to assist you as you use it.

Kaspersky Security Network

Kaspersky Security Network – a system providing an automatic transfer of reports about detected and potential threats into the centralized database. This database ensures an even faster reaction to most common threats and notification of users about virus outbreaks.

License

When you purchase Kaspersky Internet Security, you enter into a licensing agreement with Kaspersky Lab which governs the use of the application as well as your access to application database updates and Technical Support over a specified period of time. The term of use and other information necessary for full functionality of the application are provided in a key file.

Using the **License** function you can obtain details of the license you are using, purchase a new license or renew your current license.

Support

All registered Kaspersky Internet Security users can take advantage of our technical support service. In order to learn where exactly you can receive technical support, use the Support function.

By following the corresponding links you can access Kaspersky Lab product users' forum, send an error report to Technical Support, or application feedback by completing a special online form.

You also have access to online Technical Support, Personal User Cabinet Services; and our personnel will be always happy to provide you with telephone support for Kaspersky Internet Security.

HEURISTIC ANALYSIS

Heuristics are used in some real-time protection components, such as File Anti-Virus, Mail Anti-Virus, and Web Anti-Virus, and in virus scans.

Of course, scanning using the signature method with a database created previously containing a description of known threats and methods for treating them will give you a definite answer regarding whether a scanned object is malicious and what dangerous program class it is classified as. The heuristic method, unlike the signature method, is aimed at detecting typical behavior of operations rather than malicious code signatures that allow the program to make a conclusion on a file with a certain likelihood.

The advantage of heuristic analysis is that you do not have to update the database before scanning. Because of this, new threats are detected before virus analysts have encountered them.

However, there are methods for circumventing heuristics. One such defensive measure is to freeze malicious code activity the moment heuristic scanning is detected.

Note

Using a combination of various scanning methods ensures greater security.

In the event of a potential threat the heuristic analyzer emulates object execution in the secure virtual environment of the application. If suspicious activity is discovered as the object executes, the object will be deemed malicious and will not be allowed to run on the host or a message will be displayed requesting further instructions from the user:

- Quarantine new threat to be scanned and processed later using updated databases
- Delete the object
- Skip (if you are positive that the object cannot be malicious).

To use heuristic methods, check **Use heuristic analyzer**. To do so, move the slider to one of these positions: Shallow, Medium, or Detailed. The level of detail of the scan provides the balance between the thoroughness, and hence the quality, of the scan for new threats and the load on operating system resources, as well as the duration of the scan. The higher you set the heuristics level, the more system resources the scan will require, and the longer it will take.

Warning!

New threats detected using heuristic analysis are quickly analyzed by Kaspersky Lab, and methods for disinfecting them are added to the hourly database updates.

If you regularly update your databases, you will be maintaining the optimal level of protection for your computer.

HARDWARE AND SOFTWARE SYSTEM REQUIREMENTS

To ensure normal functioning of the application the computer must conform to the following minimum requirements:

General requirements:

- 75 MB free hard drive space.
- CD-ROM (for installation of the application from the installation CD).
- A mouse.
- Microsoft Internet Explorer 5.5 or higher (for updating application's bases and software modules via Internet).
- Microsoft Windows Installer 2.0.

Microsoft Windows XP Home Edition (SP2 or above), Microsoft Windows XP Professional (SP2 or above), Microsoft Windows XP Professional x64 Edition:

- Intel Pentium 300 MHz processor or higher (or a compatible equivalent).
- 256 MB free RAM.

Microsoft Windows Vista Starter x32, Microsoft Windows Vista Home Basic, Microsoft Windows Vista Home Premium, Microsoft Windows Vista Business, Microsoft Windows Vista Enterprise, Microsoft Windows Vista Ultimate:

- Intel Pentium 800 MHz 32-bit (x86) / 64-bit (x64) processor or higher (or a compatible equivalent).
- 512 MB free RAM.

THREATS TO COMPUTER SECURITY

A considerable threat to the computer security is imposed by threat applications. Additionally, such threat is imposed by spam, phishing, hacker attacks and adware ad banners. These threats are related to internet use.

IN THIS SECTION:

Threat applications 16

Internet threats 35

THREAT APPLICATIONS

Kaspersky Lab's application can detect hundreds thousands of malware programs that may reside on your computer. Some of these programs impose a greater threat for your computer; others are only dangerous when certain conditions are met. After the application detects a malware application, it classifies it and assigns to it a danger level (high or medium).

Kaspersky Lab's virus analysts distinguish two main categories: *malware programs and potentially unwanted programs.*

Malware programs (see page 17) (Malware) are created with the purpose to damage a computer and its user, for example, to steal, block, modify or erase information, disrupt operation of a computer or a computer network.

Potentially unwanted programs (see page 29) (PUPs), unlike malware programs, are not intended solely to inflict damage.

Virus Encyclopedia (http://www.viruslist.com/en/viruses/encyclopedia) contains a detailed description of these programs.

MALICIOUS PROGRAMS

Malicious programs are created specifically to inflict harm to computers and their users: steal, block, modify or erase information, disrupt the operation of computers or computer networks.

Malware programs are divided into three subcategories: *viruses and worms, Trojans programs and malware utilities.*

Viruses and worms (see page 17) (Viruses_and_Worms) can create copies of themselves which are, in turn, capable of creating their own copies. Some of them run without user's knowledge or participation, others require actions on the user's part to be run. These programs perform their malicious actions when run.

Trojan programs (see page 20) (Trojan_programs) do not create copies of themselves, unlike worms and viruses. They sneak into a computer, for example, via e-mail or using a web browser when the user visits an "infected" website. To be launched they require user's actions and start performing their malicious actions as they run.

Malware utilities (see page 26) (Malicious_tools) are created specifically to inflict damage. However, unlike other malware programs, they do not perform malicious actions immediately as they are run and can be safely stored and run on the user's computer. Such programs have functions used to create viruses, worms and Trojan programs, arrange network attacks on remote servers, hacking computers or other malicious actions.

VIRUSES AND WORMS

Subcategory: viruses and worms (Viruses_and_Worms)

Severity level: high

Classic viruses and worms perform on the computer actions not allowed by the user and can create copies of themeselves which are also able of creating their own copies.

Classic virus

After a classic virus infiltrates into the system, it infects a file, activates in it, performs its malicious action and then adds copies of itself into other files.

Classic viruses reproduce only on the local resources of a certain computer, they cannot independently penetrate other computers. They can penetrate other computers only if it adds its copy into a file stored in a shared folder or on a CD or if the user forwards an e-mail messages with at infected attachment.

Code of a classic virus can penetrate various areas of a computer, operating system or application. Based on the environment, there is a distinction between *file, boot, script and macro viruses*.

Viruses can infect files using various methods. Overwriting viruses write their own code replacing the code of the file they infect and after they destroy the content of such file. The infected file stops working and cannot be disinfected. *Parasitic viruses* modify files leaving them fully or partially operating. *Companion viruses* do not modify files but create their duplicates. When such infected file is opened, its duplicate, that is the virus, will be run. There are also link viruses, (OBJ) viruses that *infect object modules*, viruses that *infect compiler libraries* (LIB), viruses that *infect original text of programs*, etc.

Worm

After it penetrates the system, the code of a network worm, similarly to the classic virus code, gets activated and performs its malicious action. The network worm received its name due to its ability to tunnel from one computer to another - without he user's knowledge - to send copies of itself through various information channels.

The major method of proliferation is the main attribute that differentiates various types of worms. The table below lists types of worms based on the method of their proliferation.

Table 1. Worms by the method of proliferation

TYPE	NAME	DESCRIPTION
IM-Worm	IM worms	These worms propagate through IM (instant messaging) clients, such as ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager or Skype. Usually such worm uses contact lists to send messages containing a link to a file with its copy on the website. When a user downloads and opens such file, the worm will be activated.

TYPE	NAME	DESCRIPTION
Email-Worm	E-mail worms	E-mail worms infect computers via e-mail. An infected message contains an attached file containing a copy of a worm or a link to such file uploaded to a website that, for example, can be hacked or be a hacker's site itself. When you open such attachment the worm gets activated; when you click the link, download and then open a file, the worm will also start performing its malicious action. After this it will continue reproduce through its copies finding other e-mail addresses and sending infected messages to them.
IRC-Worms	IM worms	Worms of this type get into computers through Internet Relay chats - service systems used to communicate with other people via internet in real-time format. This worm publishes in the internet chat a file with its copy or a link to such file. When a user downloads and opens such file, the worm will be activated.
Net-Worms	Network worms (worms residing in computer networks)	These worms are distributed via computer networks. Unlike worms of other types, network worms are propagated without the user's participation. They search in the local area networks computers using programs containing vulnerabilities. For this it sends a special network packet (exploit) containing its code or a part of such code. If there is a vulnerable computer in the network, such computer will receive such packet. Once the worm fully penetrates the computer, it gets activated.

TYPE	NAME	DESCRIPTION
P2P-Worm	File exchange worms	File exchange worms propagate through file-exchange peer-to-peer networks, such as Kazaa, Grokster, EDonkey, FastTrack or Gnutella. In order to sneak into a file exchange network, the worm copies itself into the file-exchange folder usually located on the user's computer. The file-exchange network displays information about this fact and the user can "find" the infected file in the network, like any other file, downloaded it and open it. More complex worms imitate network protocols of a specific file exchange network: they provide positive responses to search requests and offer their copies for downloading.
Worm	Other worms	Other network worms include: • Worms that distribute their copies via network resources. Using the operating system's functionality, they go through available network folders, connect to computers in the global network and attempt to open their drives for full access. Unlike computer network worms, the user has to open a file containing a copy of the worm to activate it. • Worms that do not use any method of propagation described in this table (for example, worms propagating via mobile phones).

TROJANS

Subcategory: Trojans (Trojan_programs)

Severity level: high

Unlike worms and viruses, trojan programs do not create copies of themselves. They sneak into a computer, for example, via e-mail or using a web browser when the user visits an "infected" website. Trojan programs are launched by the user and start performing their malicious actions as they run.

The behavior of different trojan programs in the infected computer may differ. The major functions of Trojans are blocking, modification and erasing of data, disruption of the operation of computers or computer networks. Besides, Trojan programs can receive and send files, run them, display messages, access web pages, download and install programs and restart the infected computer.

Intruders often use "sets" consisting of various trojan programs.

Types of trojan programs and their behavior are described in the table below.

Table 2. Types of trojan programs by behavior on the infected computer

TYPE	NAME	DESCRIPTION
Trojan-ArcBomb	Trojan programs - archive bombs	Archives; when unpacked, they increase to a size that disrupts the computer's operation. When you attempt to unpack this archive, the computer may start working slowly or "freeze" and the disk may be filled with "empty" data. "Archive bombs" are especially dangerous for file and mail servers. If an automatic incoming information processing system is used on the server, such "archive bomb" can stop the server.
Backdoor	Remote administration Trojan programs	These programs are considered the most dangerous among Trojan programs; function-wise they remind of off-the-shelf remote administration programs. These programs install themselves without the user's knowledge and give up to the intruder remote management of the computer.

TYPE	NAME	DESCRIPTION
Trojans	Trojans	Trojans include the following malicious programs: • **classic Trojan programs**; they perform only major functions of Trojan programs: blocking, modification or erasing of data, disruption of the operation of the computers or computer networks; they do not have any additional functions characteristic of other types of Trojan programs described in this table; • "**multi-purpose**" Trojan programs; they have additional functions characteristic of several types of Trojan programs.
Trojans-Ransoms	Trojan programs requiring a ransom	They "take hostage" information on the user's computer, modifying or blocking it or disrupt the operation of the computer so that the user would be unable to use the data. Then the intruder demands a ransom from the user in exchange to the promise to send the program that will restore the computer's operability.
Trojans-Clickers	Trojan-Clickers	These programs access web pages from the user's computer: they send a command to the web browser or replace web addresses stored in the system files. Using these programs the intruders arrange network attacks and increase the traffic to such sites to increase the rate of displaying ad banners.
Trojans-Downloaders	Trojan programs-downloaders	They access the intruder's web page, download from it other malware programs and install them on the user's computer; they can store the name of the downloadable malware program filename in themselves or receive it from the web page they access.

TYPE	NAME	DESCRIPTION
Trojan-Droppers	Trojan program-droppers	These programs save programs containing other Trojan programs on the computer's disk and then install them. Intruders can use Trojans-Droppers: • install a malware programs without the user's knowledge: trojans-droppers do not display any messages or do display false messages, for example, notifying about an error in the archive or about using the wrong version of the operating system; • protect another known malware program from being detected: not any anti-virus program can detect a malware program located inside a trojan-dropper.
Trojans-Notifiers	Trojans-notifiers	They notify the intruder that the infected computer is connected; and then - transfer information about such computer to the intruder, including: IP address, number of an open port or the e-mail address. They communicate to the intruder by e-mail, via FTP, by accessing the intruder's web page or using other methods. Trojans-notifiers are often used in sets comprised of various Trojan programs. They notify the intruder that other Trojan programs are successfully installed on the user's computer.
Trojans-Proxies	Trojans-Proxies	They allow the intruder to access web pages anonymously using the user's computer and are often used to send spam.

TYPE	NAME	DESCRIPTION
Trojans-PSWs	Trojans stealing passwords	Trojans stealing passwords (Password Stealing Ware); they steal users' accounts, for example, software registration information. They find confidential information in the system files and in the registry and send it to their developer by e-mail, via FTP, accessing the intruder's website or using other methods. Some of these Trojan programs fall into specific types described in this table. These are Trojan programs stealing banking account information (Trojans-Bankers), Trojan programs stealing personal data of the users of IM client programs (Trojans-IMs) and Trojan programs stealing data from the users of network games (Trojans-GameThieves).
Trojans-Spies	Trojan spy programs	These programs are used for spying after the user: they collect information about the user's actions on the computer, for example, they intercept data entered by the user from the keyboard, make snapshots of the screen and collect lists of active applications. After they receive this information, they transfer it to the intruder by e-mail, via FTP, by accessing the intruder's website or using other methods.
Trojans-DDoS	Trojan programs - network attacks	They send numerous requests from the user's computer to the remote server. The server will then exhaust its resources for processing requests and will stop functioning (Denial-of-Service (DoS)). These programs are often used to infect multiple computers in order to attack the server from them.

TYPE	NAME	DESCRIPTION
Trojans-IMs	Trojan programs stealing personal data of the IM client users	These programs steal numbers and passwords of the IM client users (instant messaging programs), such as ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager or Skype. Then they transfer information to the intruder by e-mail, via FTP, by accessing the intruder's website or using other methods.
Rootkits	Rootkits	These programs conceal other malware programs and their activity and, thus, extend the existence of such programs in the system; they hide files or processes in the memory of an infected computer or register keys run by the malware programs or conceal data exchange between the applications installed on the user's computer and other computes in the network.
Trojans-SMS	Trojan programs - SMS messages	These programs infect mobile phones and send from the sms messages to numbers for which the user of the infected phone is charged.
Trojans-GameThieves	Trojan programs stealing personal data of the users of network games.	These programs steal user account information of network game users; they then transfer this information to the intruder by e-mail, via FTP, by accessing the intruder's website or using other methods.
Trojans-Bankers	Trojan programs stealing banking account information	These programs steal banking account information or electronic/digital money account information; they transfer data to the intruder by e-mail, via FTP, by accessing the intruder's website or using other methods.

TYPE	NAME	DESCRIPTION
Trojans-Mailfinders	Trojan programs that collect e-mail addresses	These programs collect e-mail addresses on the computer and transfer them to the intruder by e-mail, via FTP, by accessing the intruder's website or using other methods. The intruder can use collected addresses to send spam.

MALICIOUS UTILITIES

Subcategory: malicious utilities (Malicious_tools)

Severity level: medium

These utilities are designed specifically to inflict damage. However, unlike other malware programs, they do not perform malicious actions immediately as they are run and can be safely stored and run on the user's computer. Such programs have functions used to create viruses, worms and Trojan programs, arrange network attacks on remote servers, hacking computers or other malicious actions.

There are many types of malware utilities with different functions. Their types are described in the table below.

Table 3. Malware utilities by functions

TYPE	NAME	DESCRIPTION
Constructor	Constructors	Constructors are used to create new viruses, worms and Trojan programs. Some constructors have standard windows interface allowing to select the type of the malicious program to be created, the method this program will use to resist debugging and other properties..
Dos	Network attacks	They send numerous requests from the user's computer to the remote server. The server will then exhaust its resources for processing requests and will stop functioning (Denial-of-Service (DoS)).

TYPE	NAME	DESCRIPTION
Exploit	Exploits	Exploit is a set of data or a program code used application's vulnerabilities procecced to perfom a malicious action on the computer. For example, exploits can write or read files or access "infected" web pages. Different exploits use vulnerabilities of different applications or network services. An exploit is transferred via the network to multiple computers in the form of a network packet searching for computers with vulnerable network services. Exploit contained in a DOC file uses vulnerabilities of text editors. It can start perform functions programmed by the intruder when the user opens an infected file. An exploit contained in an e-mail message searches for vulnerabilities in e-mail client programs; it can start performing its malicious action as soon as the user opens an infected message in this program. Exploits are used to distribute net worms (Net-Worm). Exploits-Nukers are network packets that make computers inoperative.
FileCryptors	File Cryptors	File cryptors decrypt other malicious programs in order to hide them from anti-virus applications.

TYPE	NAME	DESCRIPTION
Flooders	Programs used for flooding networks	They send a great number of messages via network channels. These channels include, for example, programs used for flooding internet relay chats. However, this type of malware does not include programs flooding e-mail traffic and IM and SMS channels. Such programs are classified as individual types described in the table below (Email-Flooder, IM-Flooder and SMS-Flooder).
HackTools	Hacking Tools	Hacking tools are used to hack computer on which they are installed or to arrange attacks on another computer (for example, to add other system users without permission; clear the system logs in order to conceal any traces of they presence in the system). They include some sniffers which perform malicious functions, for example, intercept passwords. Sniffers are programs which allow viewing network traffic.
not-virus:Hoax	Hoax programs	These programs scare the user with virus-like messages: they can "detect" a virus in a clean file or display a message about disk formatting which will not take place.
Spoofers	Spoofers	These programs send messages and network request with a fake sender's address. Intruders use spoofers in order, for example, to pretend to be a sender.
VirTools	They are tools used to create modifications of malware programs	They make it possible to modify other malware programs in order to hide them from anti-virus applications.

TYPE	NAME	DESCRIPTION
Email-Flooders	Programs for flooding e-mail e-mail addresses	These programs send numerous messages to e-mail addresses (flood them). Due to the large flow of messages, the users are unable to view non-spam incoming messages.
IM-Flooders	Programs used for flooding IM programs	These programs send numerous messages to IM client users (instant messaging programs), such as ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager or Skype. Due to the large flow of messages, the users are unable to view non-spam incoming messages.
SMS-Flooders	Programs used for flooding with SMS text messages	These programs send numerous SMS messages to mobile phones.

POTENTIALY UNWANTED PROGRAMS

Potentially unwanted programs, unlike malware programs, are not intended solely to inflict damage. However they can be used to breach the computer's security.

Potentially unwanted programs include adware, pornware and other *potentially unwanted programs*.

Adware programs (see page 30) involve display of advertising information to the user.

Pornware programs (see page 30) involve display of pornographic information to the user.

Other Riskware (see page 31) – more often than not they are useful programs used by many computer users. However, if an intruder obtains access to these programs or install them to the user's computer, such intruder can use their functionality to breach the security.

Potentially unwanted programs are installed using one of the following methods:

- They are installed by the user, individually or along with another program (for example, software developers include adware programs into freeware or shareware programs).
- They are also installed by intruders, for example they include such programs into packages with other malware programs, use "vulnerabilities" of the web browser or Trojan downloaders and droppers, when the user visits an "infected" website.

ADWARE

Subcategory: Adware

Severity level: medium

Adware programs involve display of advertising information to the user. They display ad banners in other program's interface and redirect search queries to advertising websites. Some adware programs collect and redirect to their developer marketing information about the user, for example, which sites he or she visits or which search requests he or she performs (unlike Trojan spies, these programs transfer this information with the user's permission).

PORNWARE

Subcategory: Pornware

Severity level: medium

Usually, users install such programs themselves in order to search for or download pornographic information.

Intruders also can install these programs on the user's computer in order to display ads of commercial pornographic sites and services to the user without his or her permission. To be installed, they use vulnerabilities of the operating system or web browser, Trojan downloaders and Trojan droppers.

There are three types of pornographic nature distinguished based on their functions. These types are described in the table below.

Table 4. Types of pornware programs depending on their functions

TYPE	NAME	DESCRIPTION
Porn-Dialers	Automatic dialers	These programs automatically dial pornographic phone services (they store phone numbers of such services); unlike Trojan dialers, they notify users about their actions.
Porn-Downloaders	Programs for downloading files from the Internet	These programs download to the user's computer pornographic information; unlike Trojan dialers, they notify users about their actions.
Porn-Tools	Tools	They are used to search for and display pornography; this type include special browser toolbar and special video players.

OTHER RISKWARE PROGRAMS

Subcategory: other riskware programs

Severity level: medium

Most of these programs are useful programs used by many users. They include IRC clients, dialers, file downloading programs, computer system activity monitors, utilities for working with passwords, FTP, HTTP or Telnet service internet servers.

However, if an intruder obtains access to these programs or install them to the user's computer, such intruder can use some of their functionality to breach the security.

Other riskware programs are classified depending on their functions. Their types are described in the table below.

Table 5. Types of other riskware distinguished based on their functions

TYPE	NAME	DESCRIPTION
Client-IRC	Internet chat client programs	Users install these programs to communicate through Internet Relay Charts. Intruders use them to spread malware programs.
Dialers	Automatic dialing programs	These programs can establish "hidden" phone connections via the modem.
Downloaders	Downloaders	These programs can secretly download files from websites.
Monitors	Monitors	These programs allow monitor activities of computers on which they are installed (monitor performance of applications, how they exchange data with applications on other computers, etc.)
PSWTools	Password recovery tools	These programs are used to view and recover forgotten passwords. Intruders pursue exactly the same purpose when they install them on users' computers.

TYPE	NAME	DESCRIPTION
RemoteAdmin	Remote administration programs	These programs are often used by system administrators; they provide access to the remote computer's interface to monitor and manage it. Intruders pursue exactly the same purpose when they install them on users' computers to monitor and manage them. Remote administration riskware programs are different from Trojan remote administration programs called Backdoor. Trojan programs have functions which allow them to independently infiltrate the system and install themselves; riskware programs do not have this functionality.
Server-FTP	FTP servers	These programs perform the functions of FTP servers. Intruders install them on the users' computers to obtain remote access via FTP protocol.
Server-Proxy	Proxy servers	These programs perform the functions of proxy servers. Intruders install them on the users' computers to send spam on the users' behalf.
Server-Telnet	Telnet servers	These programs perform the functions of Telnet servers. Intruders install them on the users' computers to obtain remote access via Telnet protocol.
Server-Web	Web servers	These programs perform the functions of web servers. Intruders install them on the users' computers to obtain remote access via HTTP protocol.

TYPE	NAME	DESCRIPTION
RiskTool	Local computer tools	These tools provide users with additional functionality and are used within the user's computer only (they allow hiding files or windows of active applications, closing active processes).
NetTool	Network tools	These tools provide a user of the computer on which they are installed additional functionality for managing other computers within the network (restart them, find open ports, run programs installed on these computers).
Client-P2P	Peer-to-peer client programs	These programs are used for using peer-to-peer networks. Intruders can use them to spread malware programs.
Client-SMTP	SMTP clients	These programs send e-mail messages in hidden mode. Intruders install them on the users' computers to send spam on the users' behalf.
WebToolbar	Web toolbars	These programs add their own search toolbars to other applications' toolbars.
FraudTool	Fraud programs	These programs camouflage as other real programs. For example, there are fraudulent anti-virus programs; they display messages about detection of malware programs, but they do not find or disinfect anything.

METHODS OF DETECTING INFECTED, SUSPICIOUS AND POTENTIALLY DANGEROUS OBJECTS BY THE APPLICATION

Kaspersky Lab's application detects malware programs in the objects using two methods: reactive (using databases) and proactive (using heuristic analysis).

Bases are files with records that are used to identify the presence of hundreds of thousands known threats in the detectable objects. These records contain information about the control sections of the malware programs' code and algorithms used for disinfecting objects in which these programs are contained. Kaspersky Lab's anti-virus analysts detect hundreds of new malware programs on a daily basis, create records that identify them and include them into the database updates.

If Kaspersky Lab's application detects in a detectable object sections of code that fully coincide with the control code sections of a malware program based on the information provided in the base, it will find such object infected, and, if it coincides only partially (in accordance with some conditions) – suspicious.

Using the proactive method the application can detect newest malicious programs information of which is not yet entered into the database.

Kaspersky Lab's application detects objects containing new malware programs based on their behavior. It would not be true to say that the code of such object fully or partially coincides with the code of a known malware program, but it does contain some command sequences characteristic of malware programs, such as opening a file or writing to a file or interception of interrupt vectors. The application determines for example hat a file seems to be infected with an unknown boot virus.

Objects detected using the proactive method are calledpotentially dangerous.

INTERNET THREATS

Kaspersky Lab's application uses special technologies in order to prevent the following computer security threats:

- spam unsolicited incoming mail (see section "Unsolicited incoming mail or Spam" on page 36);

- phishing (on page 36);
- hacker attacks (on page 37);
- banners display (on page 37).

SPAM OR UNSOLICITED INCOMING MAIL

Kaspersky Lab's application protects users from spam. Spam is unsolicited incoming mail often of advertising nature. Spam is an additional load on the channels and provider's mail servers. The recipient pays for the traffic created by Spam and non-spam mail travels slower. Therefore spam is illegal in many countries.

Kaspersky Lab's application scans incoming Microsoft Office Outlook, Microsoft Outlook Express and The Bat! messages and if, if it detects any message as spam, it performs actions you selected, for example, moves such messages into a special folder or deletes them.

Kaspersky Lab's application detects spam with a great degree of accuracy. It applies several Spam filtering technologies: it detects Spam based on the sender's address as well as words and phrases in the messages subject line; it detects graphic spam and uses self-training algorithm for detecting Spam based on the message text.

Anti-Spam databases contain the "black" and the "white" lists of senders' addresses, lists of words and phrases related to various categories of spam such as advertising, medicine and health, gambling, etc.

PHISHING

Phishing is a type of fraudulent Internet activity involving "fishing" from users of numbers of credit cards, pins and other personal information in order to steal their money.

Phishing is often related to internet bankers. Intruders create an exact copy of the bank they target and then send messages to its clients on it behalf. They notify them that due to the changes in or failure of the web banking software users' accounts were lost and that the user must confirm or change his or her information on the bank's website. The user clicks the link to the website created by the intruders and enter his or here personal data there.

Anti-phishing databases contain the list URLs of websites known as sites used for phishing attacks.

Kaspersky Lab's application analyzes incoming Microsoft Office Outlook and Microsoft Outlook Express messages and if it finds a link to a URL included into the databases, it marks this message as Spam. If the user opens the message and tries to follow the link, the application blocks this website.

HACKER ATTACKS

Network attack is an intrusion into a remote computer's system in order to gain control over it and cause its failure or obtain access to protected information.

Network attacks are either actions of intruders (for example, scanning ports, attempts to hack passwords) or malware programs running commands on user's behalf and transferring information to its "master" or perform other functions related to network attacks. They include some Trojan programs, DoS attacks, malicious scripts and certain types of network worms.

Network attacks are spread in the local area and global networks using vulnerabilities in the operating systems and applications. They can be transferred as individual IP data packets during network connections.

Kaspersky Lab's application stops network attacks without disrupting network connections. It uses special Firewall databases. These databases contain records identifying IP data packets characteristic of various hacking programs. The application analyzes network connections and blocks in them those IP packets it finds dangerous.

BANNERS DISPLAY

Banners or ads which are links to the advertiser's website are more often than not displayed as images. Display of banners on the website does not impose any threat to the computer's security, but is still considered an interference into the normal operation of the computer. Banner's flickering on the screen worsens working conditions decreasing efficiency. The user is distracted by irrelevant information. Following banner links increases the internet traffic.

Many organizations prohibit displaying banners in the interfaces as a part of their data security policies.

Kaspersky Lab's application blocks banners based on the URL of the website to which the banner has a link. It uses updatable Anti-Banner databases which contain the list of URLs of Russian and foreign banner networks. The application goes through the links of the website being loaded, compares them to the addresses in the databases and if it finds a certain link in one of them, it deletes the link to this address from the site and continues loading the page.

INSTALLING APPLICATION ON THE COMPUTER

The application is installed on the computer in the interactive mode using the application setup wizard.

> Warning!
>
> We recommend that you close all running applications before proceeding with the installation.

To install the application on your computer run the distribution file (file with *.exe extension).

> Note
>
> Installation of the application from the installation file downloaded via Internet is fully identical to the installation from CD.

After this the setup wizard will scan for the application installation package (file with extension *.msi) and, if such file is found, the wizard will scan for a newer version on Kaspersky Lab's internet servers. If the installation package file was not found, you will be offered to download it. Once the file is downloaded, the application setup will be started. If you cancel downloading the application installation process will be resumed in normal mode.

The setup program is implemented as a wizard. Each window contains a set of buttons to control the installation process. Provided below is the brief description of their purpose:

- **Next** – accept the action and switch to the next step of the installation process.
- **Previous** – return to the previous step of the installation process.
- **Cancel** – cancel the installation.
- **Finish** – complete the application installation procedure.

A detailed discussion of each step of the package installation is provided below.

IN THIS SECTION:

Step 1. Searching for a newer version of the application....40

Step 2. Verifying the system's conformity to the installation requirements 41

Step 3. Wizard's greeting window....41

Step 4. Viewing the License Agreement....41

Step 5. Selecting the installation type....42

Step 6. Selecting the installation folder....42

Step 7. Selecting application components to be installed....43

Step 8. Searching for other anti-virus software....44

Step 9. Final preparation for the installation 45

Step 10. Completing the installation 45

STEP 1. SEARCHING FOR A NEWER VERSION OF THE APPLICATION

Before installing the application on your computer, the wizard will access Kaspersky Lab's update servers to check whether a newer version of the application being installed exists.

If such newer version was not detected on the Kaspersky Lab's update servers, the setup wizard will be started to install the current version.

If a newer version of the application is found on the servers you will be offered to download it. If you cancel the download, the setup wizard will be started to install the current version. If you decide to install a newer version the installation files will be downloaded to your computer and the setup wizard will be automatically started to install the newer version. For more details on the installation of a newer version refer to the documentation of the corresponding application version.

STEP 2. VERIFYING THE SYSTEM'S CONFORMITY TO THE INSTALLATION REQUIREMENTS

Before installing the application on your computer the wizard will verify the conformity of the operating system and service packs installed to the software installation requirements (see section "Hardware and software system requirements" on page 14). It will also verify that the required programs are installed on your computer and that you have the rights required to install software on it.

If any of the requirements is not met, a corresponding notification will be displayed on the screen. We recommend that you install the required updates using the **Windows Update** service and the required programs before the installation of the Kaspersky Lab's application.

STEP 3. WIZARD'S GREETING WINDOW

If your system fully conform to the requirements (see section "Hardware and software system requirements" on page 14), no newer version of the application was found at Kaspersky Lab's update servers or if you cancelled installation of such newer version, the setup wizard will be started to install the current version of the application. The first dialog box of the setup wizard containing information about commencement of the application installation on your computer will then be displayed on the screen.

To proceed with the installation press the **Next** button. To cancel installation press the **Cancel** button.

STEP 4. VIEWING THE LICENSE AGREEMENT

Next wizard's dialog box contains the license agreement between you and Kaspersky Lab. Read it carefully and if you agree with all terms and conditions of the agreement, select **I accept the terms of the license agreement** and press the **Next** button. The installation will be continued.

To cancel the installation press the **Cancel** button.

STEP 5. SELECTING THE INSTALLATION TYPE

During this step you will be offered to select the installation type that suits you best:

- **Express installation**. If you select this option, the entire application will be installed on your computer with the protection settings recommended by Kaspersky Lab's experts. Once the installation is complete the Application Setup wizard will be started.
- **Custom installation**. In this case you will be offered to select the application's components you wish to install on your computer, specify folder into which the application will be installed (see section "Step 6. Selecting the installation folder" on page 42), to activate the application and configure it using a special wizard.

If you select the first option, the application installation wizard will switch directly to Step 8 *(*see section "Step 8. Searching for other anti-virus applications" on page 44). Otherwise your input or confirmation will be required at each step of the installation.

STEP 6. SELECTING THE INSTALLATION FOLDER

Note

This step of the installation wizard will be performed only if you selected the custom installation option (see section "Step 5. Selecting the installation type" on page 42).

During this step you will be offered to identify a folder on your computer into which the application will be installed. The default path is:

- **<Drive> \ Program Files \ Kaspersky Lab \ Kaspersky Internet Security 2009** – for 32-bit systems.

- **<Drive> \ Program Files (x86) \ Kaspersky Lab \ Kaspersky Internet Security 2009** – for 64-bit systems.

You can specify a different folder by pressing the **Browse** button and selecting a folder in the standard folder select dialog box or entering the path to it in the entry field provided.

Warning!

Please note that if you manually enter the full path to the installation folder, its length should not exceed 200 characters and the path should not contain special characters.

To proceed with the installation press the **Next** button.

STEP 7. SELECTING APPLICATION COMPONENTS TO BE INSTALLED

Note. This step of the installation wizard will be performed only if you selected the custom installation option (see section "Step 5. Selecting the installation type" on page 42).

In case of a custom installation you must select the application's components you wish to be installed on your computer. By default all application's components are selected for installation: protection, scan and updating components.

To make a decision which components you do not wish to install, use brief information about components. To do it select the component from the list and read information about it in the field below. Information includes a brief description of the component and the free hard drive space required for its installation.

To cancel installation of any component, open the shortcut menu by clicking the icon next to the component's name and select the **Component will not be available** item. Note that if you cancel installation of any component you will not be protected against a number of hazardous programs.

To select a component to be installed, open the shortcut menu by clicking the icon next to the component's name and select **Component will be installed on local hard drive**.

After you finished selecting components to be installed, press the **Next** button. To return to the list of components to be installed by default press the **Clear** button.

STEP 8. SEARCHING FOR OTHER ANTI-VIRUS SOFTWARE

During this step the wizard performs a search for other anti-virus programs including Kaspersky Lab's programs which may conflict with the application being installed.

If such programs were detected on your computer, the list of such programs will be displayed on the screen. You will be offered to delete them before you proceed with the installation.

You can choose whether you wish to remove them automatically or manually using the controls located below the list of detected anti-virus programs.

If the list of detected anti-virus programs includes Kaspersky Lab's 7.0 application, save the key file used for this application when you remove the application. You can use this key for the new version of the application. We also recommend saving objects stored in the quarantine and in the backup storage; these objects will be automatically moved to the quarantine of the new version and you will be able to manage them after the installation.

In case of the automatic removal of 7.0 version, information about its activation will be saved by the program and then will be used during the installation of version 2009.

Warning!

The application supports key files for versions 6.0 and 7.0. Keys used by 5.0 version applications are not supported.

To proceed with the installation press the **Next** button.

STEP 9. FINAL PREPARATION FOR THE INSTALLATION

During this step you will be offered to perform the final preparation for the installation to your computer.

During the initial and custom application installation (see section "Step 5. Selecting the installation type" on page 42) we recommend that you do not uncheck the **Enable Self-Defense before installation** box during the initial installation. If the module protection option is enabled, then, if an error occurs during the installation, it will ensure a correct installation rollback procedure. When you retry the installation we recommend that you uncheck this box.

Note

In case of a remote installation of the application via **Remote Desktop** we recommend that you uncheck the **Enable Self-Defense before installation** box. If this box is checked, the installation procedure may be performed incorrectly or not performed at all.

To proceed with the installation press the **Next** button. As the result installation files will start copying to your computer.

Warning!

During the installation process current network connection will be severed if the application package includes components for intercepting network traffic. The majority of connections terminated will be restored after some time.

STEP 10. COMPLETING THE INSTALLATION

The **Installation complete** window contains information about completing the procedure of the application installation on your computer.

If it is necessary to restart the computer to correctly complete the installation, a corresponding notification will be displayed on the screen. After the system restart the setup wizard will be automatically started.

If the system restart is not required to complete the installation, press the **Next** button to start the application configuration wizard.

APPLICATION INTERFACE

The application has a fairly simple and easy-to-use interface. This chapter will discuss its basic features in detail.

In addition to the main program interface, there are plugins for Microsoft Office Outlook (scan for viruses and spam processing), Microsoft Outlook Express (Windows Mail), The Bat! (scan for viruses and spam processing), Microsoft Internet Explorer and Microsoft Windows Explorer. The plugins expand the functionality of the applications listed above providing an ability to manage and configure components Mail Anti-Virus and Anti-Spam from the interface.

IN THIS SECTION:

Notification area icon 46

Shortcut menu 47

Main application window 49

Notifications 52

Application settings configuration window 52

NOTIFICATION AREA ICON

Immediately after the installation of the application, the application icon will appear in the Microsoft Windows taskbar notification area.

This icon is an indicator of the application's operation. It reflects the protection status and shows a number of basic functions performed by the program.

If the icon is active (color), the full protection or some of its components are running. If the icon is inactive (black and white), all protection components have been disabled.

The application icon changes depending on the operation being performed:

– e-mail being scanned.

– updating application databases and program modules.

– computer needs reboot to apply updates.

– an error has occurred in some Kaspersky Internet Security component.

The icon also provides access the basics of the program interface: shortcut menu (see section "Shortcut menu" on page 47) and main application window (see section "Main application window" on page 49).

To open the shortcut menu, right-click the application icon.

In order to open the main application window, double click the application icon. The main window always opens on section **Protection**.

If news from Kaspersky Lab is available, icon news will appear in the taskbar notification area . Double click the icon to view the news in the resulting window.

SHORTCUT MENU

You can run basic protection tasks from the context menu.

The application menu contains the following items:

- **Update** - start the application module and database updates and install updates on your computer.
- **Full computer scan** - start a complete scan of the computer for dangerous objects. Objects residing on all drives, including removable storage media, will be scanned.
- **Virus scan** - select objects and start a virus scan. By default the list contains several objects, such as **My documents** folder and mailboxes. You can complement this list by selecting objects to be scanned and start an anti-virus search.
- **Network Monitor** - view the list of network connections established, open ports, and traffic.

- **Virtual keyboard** – switching to the virtual keyboard.
- **Kaspersky Internet Security** – opening the main application window (see section "Main application window" on page 49).
- **Settings** - view and configure the application settings.
- **Activate** - activate the program. In order to obtain the status of a registered user, you must activate your application. This menu item is only available if the program is not activated.
- **About** - display window with information about the application.
- **Pause protection / Resume protection** - temporarily disable or enable the real-time protection components. This menu option does not affect the product's updates or virus scan task execution.
- **Block network traffic** - temporarily block all the computer's network connections. If you want to allow the computer to interact with the network, select this item from the context menu again.
- **Exit** - close the application (when this option is selected, the application will be unloaded from the computer's RAM).

Figure 1: Shortcut menu

If a virus scan task is running at the moment you open the shortcut menu, its name as well as its progress status (percentage complete) will be displayed in the shortcut menu. By selecting the task you can go to the main window containing a report about the current results of its execution.

MAIN APPLICATION WINDOW

The main application window can be divided into three parts:

- The top part of the window indicates your computer's current protection status.

Figure 2: Current status of the computer protection

There are three possible protection statuses, each of these statuses is visually displayed by a certain color similarly to the traffic lights. Green color indicates that protection of your computer is at the correct level, yellow and red colors warn about the presence of various security threats in settings configuration or in operation of the application. In addition to malware programs, threats include obsolete application bases, some disabled protection components, minimum application settings selected, etc.

The security threats must be eliminated as they appear. To obtain detailed information about them and for their quick elimination use the **Fix it now** link (see figure above).

- The left-hand part of the window - navigation bar - is used to quickly switch to using any application function, execution of anti-virus scan task, updating task, etc.

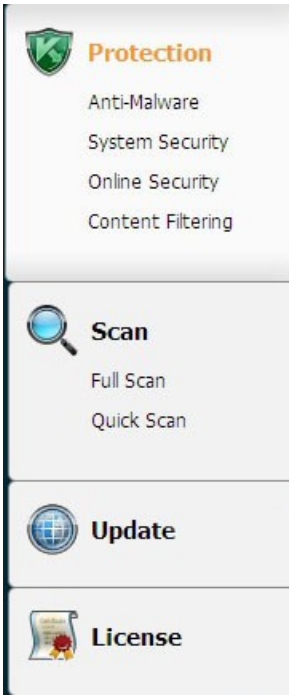

Figure 3: Left part of the main window

- The right-hand part of the window contains information about the application function selected in the left-hand part and is used to configure settings of such functions and to provide tools for performing anti-virus scan tasks, downloading updates, etc.

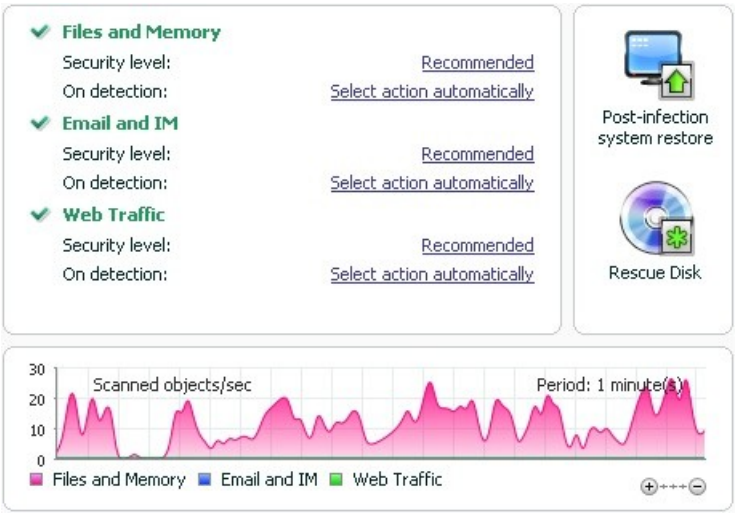

Figure 4: Informational part of the main window

You can also use buttons:

- **Settings** - to switch to the application's settings.
- **Help** - to switch to the application Help system.
- **Detected** - switching to the list of harmful objects detected as the result of the operation of any component or an anti-virus scan task completed and to viewing the detailed statistics of the application's operation results.
- **Reports** - switching to the list of events occurred during the application's operation.
- **Support** - to open the window containing information about the system and links to Kaspersky Lab's information resources (Technical Support service site, forum).

Note

You can change the appearance of the application by creating and using your own graphics and color schemes.

NOTIFICATIONS

If events occur in the course of the application's operation special notifications will be displayed on the screen in the form of pop-up messages above the application icon in the Microsoft Windows task bar.

Depending on the degree of criticality of the event regarding computer security, you might receive the following types of notifications:

- **Alert**. A critical event has occurred; for instance, a virus or dangerous activity has been detected on your system. You should immediately decide how the program should react. This type of notification is in red.
- **Warning**! A potentially dangerous event has occurred. For instance, potentially infected files or suspicious activity has been detected on your system. You must instruct the program depending on how dangerous you think this event is. This type of notification is in yellow.
- **Note**: This notification tells you about events that are not critical. This type, for example, includes notifications related to the operation of the **Content Filtering** component. Information notifications have green color.

APPLICATION SETTINGS CONFIGURATION WINDOW

The application settings window can be opened from main application window the (see section "Main application window" on page 49) or shortcut menu (see section "Shorctut menu" on page 47) of the application. To call up this window, click the **Settings** link in the top part of the main application window or select an appropriate option on the application shortcut menu.

The settings configuration window consists of two parts:

- the left-hand part of the window provides access to the application components, virus scan tasks, updating tasks, etc.;
- the right part of the window contains a list of settings for the component, task, etc. selected in the left part of the window.

GETTING STARTED

One of the main goals of the Kaspersky Lab specialists in making Kaspersky Internet Security was to provide optimum configuration for all the program's options. This makes it possible for the user with any level of computer literacy to ensure protection of his or her computer immediately after installation without spending hours on the settings.

For the user's convenience, we have brought the preliminary configuration stages together in the unified Initial Setup Wizard interface that starts as soon as the program is installed. By following the wizard's instructions, you can activate the application, configure settings for updates, restrict access access to the program using a password and perform other settings.

Your computer can be infected with malware before the application is installed. To detect malware programs run computer scan (see section "Anti-Virus computer scan" on page 57).

As the result of the malware operation and system failures the settings of your computer can be corrupted. Run Security analysis wizard in order to find the vulnerabilities of the installed software and anomalies of the system settings.

By the moment of the application databases included into the database package can become outdated. Start the Update the applicationupdating the application (if it was not done using the setup wizard or automatically immediately after the application is installed).

The Anti-Spam component included into the application structure uses a self-training algorithm to detect unwanted messages. Start the Anti-Spam training wizard to configure the component to work with your correspondence.

After the completion of the actions described above the application will be ready for the operation. In order to evaluate the level of protection of your computer use security management wizard (see section "Security Management" on page 59).

IN THIS SECTION:

Selecting network type 55

Updating the application 56

Security analysis 56

Scanning computer for viruses 57

Participating in Kaspersky Security Network 58

Security management 59

Pausing protection 61

SELECTING NETWORK TYPE

After the application is installed, the Firewall component will analyze the active network connections on your computer. Each network connection will be assigned a status determining the allowed network activities.

If you selected the interactive mode of Kaspersky Internet Security operation, a notification will be displayed each time a network connection is established. You can select the status for new networks in the notification window:

- Public network - for network connections with the status access to your computer from the outside is not allowed. For this networks access to public folders and printers is also allowed. This status is recommended to assign to the Internet network.
- Local network - for the network connections with such status access to public folders and network printers is allowed. It is recommended to assign this status to protected local networks, for example, a corporate network.
- Trusted network - for the network connections with this status any activities are allowed. It is recommended to assign only for the absolutely security areas.

For each network status Kaspersky Internet Security includes the set of rules for managing the network activities. Later you can change the network status specified once it is detected for the first time.

UPDATING THE APPLICATION

Warning!

You will need a connection to the Internet to update Kaspersky Internet Security.

Kaspersky Internet Security includes databases containing threat signatures, examples of phrases characteristic of spam and description of network attacks. However, at the moment of the application installation the databases can become obsolete since Kaspersky Lab updates databases and application modules on a regular bases.

You can select the updating launch mode during the application setup wizard operation. By default, Kaspersky Internet Security automatically checks for updates on the Kaspersky Lab servers. If the server contains a fresh set of updates, Kaspersky Internet Security will download and install them in the silent mode.

In order to maintain the protection of your computer in the up-to-date status we recommend that you update Kaspersky Internet Security immediately after the installation.

- *To update Kaspersky Internet Security manually,*

  1. Open main application window.
  2. Select the **Update** section in the left window side.
  3. Press the **Start update** button.

SECURITY ANALYSIS

As the result of unwanted activities on your computer which can be a result of system failures or of the activites of malware programs the settings of your operating system can become corrupted. Additionally, applications installed on your computer can have vulnerabilities used by intruders to inflict damades to your computer.

In order to detect and eliminate such security problem, Kaspersky Lab's experts recommend that you launch Security Analysis Wizard after you have installed the application. The security analysis wizard searches for vulnerabilities in the installed applications and for the damages and anomalies in the operating system's and the browser's settings.

- *To start the wizard:*

  1. Open main application window.

  2. In the left part of the window select **System Security**.

  3. Start the **Security Analyzer** task.

SCANNING COMPUTER FOR VIRUSES

Developers of malware make every effort to conceal the actions of their programs, therefore you may not notice the presence of malware programs in your computer.

Once application is installed on your computer, it automatically performs the **Quick scan** task on your computer. This task searches for and neutralizes harmful programs in objects loaded at the operating system startup.

Kaspersky Lab's specialists also recommend that you perform the **Full scan** task.

- *To start / stop a anti-virus scan task:*

  1. Open main application window.

  2. In the left-hand part of the window select **Scan** (**Full scan**, **Quick scan**) section.

  3. Click **Start scan** to start the scan. If you need to stop the task's execution click **Stop scan** while the task is in progress.

PARTICIPATING IN KASPERSKY SECURITY NETWORK

A great number of new threats appear worldwide on an everyday basis. In order to facilitate gathering the statistics about new threat types, their source and developing the method to be used for their elimination, Kaspersky Lab allows you to use the Kaspersky Security Network service.

The use of Kaspersky Security Network involves sending the following information to Kaspersky Lab:

- A unique identifier assigned to your computer by the application. This identifier characterizes the hardware settings of your computer and does not contain any information.
- Information about threats detected by the application's components. Information structure and contents depends on the type of the threat detected.
- System information: operating system's version, installed service packs, downloadable services and drivers, browser and mail client versions, browser extensions, number of the Kaspersky Lab's application installed.

Kaspersky Security Network also gathers extended statistics including information about:

- executable files and signed applications downloaded on your computer,
- applications run on your computer.

The statistical information is sent once the application updated is complete.

Warning!

Kaspersky Lab guarantees that no gathering and distribution of users' personal data is performed within Kaspersky Security Network.

- To configure the statistics sending settings:

  1. Open the application setting window.
  2. Select the **Feedback** section in the left part of the window.

3. Check the **I agree to participate in Kaspersky Security Network** box to confirm your participation in Kaspersky Security Network. Check the **I agree to send extended statistics within the framework of Kaspersky Security Network** box in order to confirm your consent to send extended statistics.

SECURITY MANAGEMENT

Problems in the computer protection are indicated by Main application window computer protection status through the change of the color of the protection status icon and of the panel in which this icon is located. Once problems appear in the protection system, we recommend fixing them immediately.

Figure 5: Current status of the computer protection

You can view the list of problems occurred, their description and the possible solutions on the **Status** tab (see figure below) that opens by clicking the **Fix it now** link (see figure above).

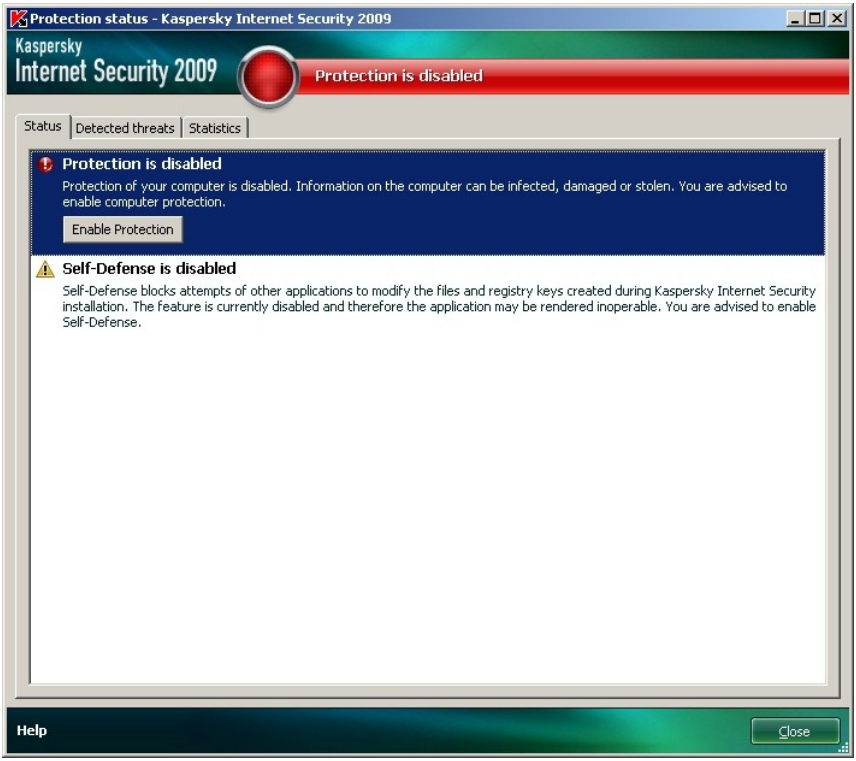
Protection status - Kaspersky Internet Security 2009
Kaspersky
Internet Security 2009
Protection is disabled
Status
Detected threats
Statistics
Protection is disabled
Protection of your computer is disabled. Information on the computer can be infected, damaged or stolen. You are advised to enable computer protection.
Enable Protection
Self-Defense is disabled
Self-Defense blocks attempts of other applications to modify the files and registry keys created during Kaspersky Internet Security installation. The feature is currently disabled and therefore the application may be rendered inoperable. You are advised to enable Self-Defense.
Help
Close

Figure 6: Solving security problems

You can view the list of existing problems. Problems are listed based on how crucial it is to solve them: first - most critical problems, that is problems with the red status icon, then - less important - the yellow status icon and the information messages come last. A detailed description is provided for each problem and the following actions are available:

- *Eliminate immediately*. Using the corresponding buttons, you can switch to fixing of the problem, which is the recommended action.
- *Postpone elimination*. If, for any reason, the immediate elimination of the problem is not possible, you can put off this action and return to it later. To do it use the **Hide message** button.

Note that this option is not available for serious problems. Such problems include, for example, malicious objects that were not disinfected, crashes of one or several components, or corruption of the program files.

In order for the hidden messages to re-appear in the general list, check the **Show hidden messages** box.

PAUSING PROTECTION

Pausing of protection means temporary disabling of all protection components for a certain period of time.

- *To pause the protection of your computer:*

1. Select the **Pausing Protection** item from the ***shortcut menu*** of the application (see section "Shorctut menu" on page 47).

2. In the **Pause protection** window that opens, select the period of time after which you want the protection to be enabled:

   - **In <time interval>** - protection will be enabled after the time interval specified elapces. Use the dropdown menu to select the time interval value.

   - **After restart** - protection will be enabled after the system restart (provided that the mode providing for application launch when the computer is turned on is enabled).

   - **Manually** - protection will be enabled only after you start it manually. To enable protection, select Resume protection from the application's shortcut menu.

As a result of temporarily disabling protection, all protection components will be paused. This is indicated by:

- Inactive (gray) names of the disabled components in the **Protection** section of the main window.

- Inactive (gray) application icon (see section "Notification Area Icon" on page 46) in the system panel.

- The red color of the status icon and of the main application window's panel.

If network connections were established at the moment when the protection was paused, a notification about breaking these connections will be displayed.

VALIDATING APPLICATION SETTINGS

After the application has been installed and configured, you can verify whether the application is configured correctly using a test "virus" and its modifications. A separate test will be performed for each protection component / protocol.

IN THIS SECTION:

Test "virus" EICAR and its modifications 63

Testing the HTTP traffic protection 67

Testing the SMTP traffic protection 67

Validating File Anti-Virus settings 68

Validating virus scan task settings 69

Validating Anti-Spam settings 69

TEST "VIRUS" EICAR AND ITS MODIFICATIONS

This test "virus" was specially designed by eicar (The European Institute for Computer Antivirus Research) for testing anti-virus products.

The test "virus" IS NOT A VIRUS because it does not contain code that can harm your computer. However, most anti-virus products manufacturers identify this file as a virus.

> Warning!
>
> Never use real viruses for testing the operation of an anti-virus product!

You can download this test "virus" from the official website of the EICAR organization at: http://www.eicar.org/anti_virus_test_file.htm.

Note

Before you download the file, you have to disable the anti-virus protection because otherwise the application would identify and process file *anti_virus_test_file.htm* as an infected object transferred via HTTP protocol.

Do not forget to enable the anti-virus protection immediately after you download the test "virus".

The application identifies the files downloaded from **EICAR** site as an infected object containing a virus that **cannot be disinfected** and performs actions specified for such object.

You can also use modifications of the standard test "virus" to verify the operation of the application. In order to do it, change the content of the standard "virus" by adding one of the prefixes to it (see table below). To create modifications of the test "virus" you can use any text or hypertext editor, for example **Microsoft Notepad**, **UltraEdit32**, etc.

Warning!

You can test the correctness of the operation of the anti-virus application using the modified EICAR "virus" only if your anti-virus bases were last updated on or after October 24, 2003 (October, 2003 cumulative updates).

The first column contains the prefixes that need to be added to the beginning of the string for a standard test "virus". The second column lists all possible values of the status that anti-virus assigns to the object based on the results of the scan. The third column contains information about the processing of objects with the specified status by the application. Please note that actions to be performed with the objects will be determined by the values of the application's settings.

After you have added the prefix to the test "virus", save the new file under a different name, for example: *eicar_dele.com*. Assign similar names to all modified "viruses".

Table 6. Modifications of the test "virus"

Prefix	Object status	Object processing information
No prefix, standard test virus	**Infected**. Infected.Object contains code of a known virus. Disinfection is not possible.	The application identifies the object as a non-disinfectible virus. An error occurs at the attempt to disinfect the object; the action assigned to be performed with non-disinfectible objects will be applied.
CORR–	Corrupted.	The application could access the object but was unable to scan it because the object is corrupted (for example, the file structure is corrupted or due to an invalid file format). Information about the object processing can be found in the report about the application operation.
WARN–	**Suspicious**. Suspicious.Object contains code of an unknown virus. Disinfection is not possible.	Object has been found suspicious by the heuristic code analyzer. At the time of detection, the Anti-Virus threat signature databases contain no description of the procedure for treating this object. You will receive a notification once such object is detected.
SUSP–	**Suspicious**. Suspicious.Object contains modified code of a known virus. Disinfection is not possible.	The application detected a partial correspondence of a section of object code with a section of code of a known virus. At the time of detection, the Anti-Virus threat signature databases contain no description of the procedure for treating this object. You will receive a notification once such object is detected.

Prefix	Object status	Object processing information
ERRO–	Scanning error:	An error occurred during a scan of an object. Application was unable to obtain access to the object: the object's integrity was breached (for example, no end to a multi-volume archive) or there is no connection to it (if the object being scanned is located on a network drive). Information about the object processing can be found in the report about the application operation.
CURE–	**Infected**. Infected.Object contains code of a known virus. Disinfectible.	Object contains a virus that can be disinfected. The application will disinfect the object; the text of the "virus" body will be replaced with word CURE. You will receive a notification once such object is detected.
DELE–	**Infected**. Infected.Object contains code of a known virus. Disinfection is not possible.	The application identifies the object as a non-disinfectible virus. An error occurs at the attempt to disinfect the object; the action assigned to be performed with non-disinfectible objects will be applied. You will receive a notification once such object is detected.

TESTING THE HTTP TRAFFIC PROTECTION

- *In order to verify detection of viruses in the data stream transferred via HTTP protocol, do the following:*

  try to download a test "virus" from the official website of the EICAR organization at: http://www.eicar.org/anti_virus_test_file.htm.

When attempting to download the test "virus", Kaspersky Internet Security will detect this object, identify it as an infected object that cannot be disinfected, and will perform an action specified in the HTTP traffic settings for this type of objects. By default, when you attempt to download the test "virus" connection with the website will be terminated and the browser will display a message informing the use that this object is infected with virus EICAR-Test-File.

TESTING THE SMTP TRAFFIC PROTECTION

In order to detect viruses in the data streams transferred using SMTP protocol, you can use a mail system that uses this protocol to transfer data.

Note

We recommend that you test how Kaspersky Internet Security handles incoming and outgoing e-mail messages including both the body of the message and the attachments. In order to test detection of viruses in the body of the message, copy the text of the standard test "virus" or of the modified "virus" into the body of the message.

- *To do this:*

  1. Create a **Plain text** format message using a mail client installed on your computer.

> Note
>
> Message that contains a test virus will not be scanned if it is created in the RTF or HTML format!

2. Copy the text of the standard or modified "virus" in the beginning of the message or attach a file containing the test "virus" to the message.

3. Send the message to the administrator.

The application will detect the object and identify it as infected. Sending of a message containing an infected object will be blocked.

VALIDATING FILE ANTI-VIRUS SETTINGS

- *In order to verify the correctness of the File Anti-Virus configuration, do the following:*

  1. Create a folder on a disk, copy the test virus downloaded from the organization's official website (http://www.eicar.org/anti_virus_test_file.htm), and the modifications of the test virus that you created.

  2. Allow all events to be logged so the report file retains data on corrupted objects and objects not scanned because of errors.

  3. Run the test "virus" or its modification file.

The File Anti-Virus will intercept the call to the file, will scan the file and will perform the action specified in the settings. By selecting various actions to be performed with the detected object, you will be able to perform a full check of the component's operation.

You can view information about the results of the File Anti-Virus operation in the report about the component's operation.

VALIDATING VIRUS SCAN TASK SETTINGS

- *In order to verify the correctness of the anti-virus scan task configuration, do the following:*

    1. Create a folder on a disk, copy the test virus downloaded from the organization's official website (http://www.eicar.org/anti_virus_test_file.htm), and the modifications of the test virus that you created.

    2. Create a new virus scan task and select the folder, containing the set of test "viruses" as the objects to scan.

    3. Allow all events to be logged so the report file retains data on corrupted objects and objects not scanned because of errors.

    4. Run the virus scan task.

When the scan task is running, actions specified in the task settings will be performed as suspicious or infected objects are detected. By selecting various actions to be performed with the detected object, you will be able to perform a full check of the component's operation.

You can view the full information about the results of the task in the report on the component's operation.

VALIDATING ANTI-SPAM SETTINGS

You can use a test message identified as SPAM to test the anti-spam protection.

The body of the test message must contain the following line:

```
Spam is bad do not send it
```

After this message is received on the computer, the application will scan it, assign the spam status to the message and will perform the action specified for the object of this type.

KASPERSKY SECURITY NETWORK DATA COLLECTION STATEMENT

INTRODUCTION

PLEASE READ THIS DOCUMENT CAREFULLY. IT CONTAINS IMPORTANT INFORMATION THAT YOU SHOULD KNOW BEFORE CONTINUING TO USE OUR SERVICES OR SOFTWARE. BY CONTINUING TO USE KASPERSKY LAB SOFTWARE AND SERVICES YOU WILL BE DEEMED TO HAVE ACCEPTED THIS KASPERSKY LAB' Data Collection STATEMENT. We reserve the right to modify this Data Collection Statement at any time by posting the changes on this page. Please check the revision date below to determine if the policy has been modified since you last reviewed it. Your continued use of any portion of Kaspersky Lab's Services following posting of the updated Data Collection Statement shall constitute your acceptance of the changes.

Kaspersky Lab and its affiliates (collectively, "***Kaspersky Lab***") has created this Data Collection Statement in order to inform and disclose its data gathering and dissemination practices for Kaspersky Anti-Virus and Kaspersky Internet Security.

Word from Kaspersky Lab

Kaspersky Lab has a strong commitment to providing superior service to all of our customers and particularly respecting your concerns about Data Collection. We understand that you may have questions about how Kaspersky Security Network collects and uses information and data and we have prepared this statement to inform you of the Data Collection principles that govern the Kaspersky Security Network (the "***Data Collection Statement***" or "***Statement***").

This Data Collection Statement contains numerous general and technical details about the steps we take to respect your Data Collection concerns. We have organized this Data Collection Statement by major processes and areas so that you can quickly review the information of most interest to you. The bottom line is that meeting your needs and expectations forms the foundation of everything we do - including protecting your Data Collection.

The data and information is collected by Kaspersky Lab and if after reviewing this Data Collection Statement you have any questions or Data Collection concerns please send an e-mail to support@kaspersky.com.

What is Kaspersky Security Network?

Kaspersky Security Network service allows users of Kaspersky Lab security products from around the world to help facilitate identification and reduce the time it takes to provide protection against new ("in the wild") security risks targeting your computer. In order to identify new threats and their sources and to help improve user security and product functionality, Kaspersky Security Network collects selected security and application data about potential security risks targeting your computer and submits that data to Kaspersky Lab for analysis. **Such information contains no personally identifiable information about the user and is utilized by Kaspersky Lab for no other purposes but to enhance its security products and to further advance solutions against malicious threats and viruses. In case of accidental transmission of any personal data of the user, Kaspersky Lab shall keep and protect it in accordance with this Data Collection Statement**.

By participating in Kaspersky Security Network, you and the other users of Kaspersky Lab security products from around the world contribute significantly to a safer Internet environment.

Legal Issues

Kaspersky Security Network may be subject to the laws of several jurisdictions because its services may be used in different jurisdictions, including the United States of America. Kaspersky Lab shall disclose personally identifiable information without your permission when required by law, or in good-faith belief that such action is necessary to investigate or protect against harmful activities to Kaspersky Lab guests, visitors, associates, or property or to others. As mentioned above, laws related to data and information collected by Kaspersky Security Network may vary by country. For example, some personally identifiable information collected in the European Union and its Member States is subject to the EU Directives concerning personal data, Privacy and electronic communications, including but not limited to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of Privacy in the electronic communications sector and Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and the subsequent legislation adopted in the EU Member States, the European Commission Decision 497/2001/EC on standard contractual clauses (personal data transferred to third countries) and the subsequent legislation adopted in the EC Member States.

Kaspersky Security Network shall duly inform the users concerned, when initially collecting the above-mentioned information, of any sharing of such information, notably for use for business development and shall allow these Internet users to **opt in** (in the EC Member States and other countries requiring opt-in procedure)

or opt-out (for all the other countries) on-line from the commercial use of this data and/or the transmission of this data to third parties.

Kaspersky Lab may be required by law enforcement or judicial authorities to provide some personally identifiable information to appropriate governmental authorities. If requested by law enforcement or judicial authorities, we shall provide this information upon receipt of the appropriate documentation. Kaspersky Lab may also provide information to law enforcement to protect its property and the health and safety of individuals as permitted by statute.

Declarations to Personal Data Protection Member States authorities shall be made according to the subsequent EU Member States legislation in force. Information about such declarations shall be accessible on the Kaspersky Security Network services.

COLLECTED INFORMATION

Data We Collect

The Kaspersky Security Network service will collect and submit core and extended data to Kaspersky Lab about potential security risks targeting your computer. The data collected includes:

Core data

- information about your computer hardware and software, including operating system and service packs installed, kernel objects, drivers, services, Internet Explorer extensions, printing extensions, Windows Explorer extensions, downloaded program files, active setup elements, control panel applets, host and registry records, IP addresses, browser types, e-mail clients and the version number of the Kaspersky Lab product, that is generally not personally identifiable;

- a unique ID that is generated by the Kaspersky Lab product to identify individual machines without identifying the user and which does not contain any personal information;

- information about the status of your computer's antivirus protection, and data on any files or activities suspected of being malware (e.g., virus name, date/time of detection, names/paths and size of infected files, IP and port of network attack, name of the application suspected of being malware). Please note that the above referenced collected data does not contain personally identifiable information.

Extended data

- Information about digitally signed applications downloaded by the user (URL, file size, signer name)

- Information about executable applications (size, attributes, date created, information about PE headers, region, name, location, and compression utility used).

Securing the Transmission and Storage of Data

Kaspersky Lab is committed to protecting the security of the information it collects. The information collected is stored on computer servers with limited and controlled access. Kaspersky Lab operates secure data networks protected by industry standard firewall and password protection systems. Kaspersky Lab uses a wide range of security technologies and procedures to protect the information collected from threats such as unauthorized access, use, or disclosure. Our security policies are periodically reviewed and enhanced as necessary, and only authorized individuals have access to the data that we collect. Kaspersky Lab takes steps to ensure that your information is treated securely and in accordance with this Statement. Unfortunately, no data transmission can be guaranteed secure. As a result, while we strive to protect your data, we cannot guarantee the security of any data you transmit to us or from our products or services, including without limitation Kaspersky Security Network, and you use all these services at your own risk.

The data that is collected may be transferred to Kaspersky Lab servers and Kaspersky Lab has taken the necessary precautions to ensure that the collected information, if transferred, receives an appropriate level of protection We treat the data we collect as confidential information; it is, accordingly, subject to our security procedures and corporate policies regarding protection and use of confidential information. After collected data reaches Kaspersky Lab it is stored on a server with physical and electronic security features as customary in the industry, including utilization of login/password procedures and electronic firewalls designed to block unauthorized access from outside of Kaspersky Lab. Data collected by Kaspersky Security Network covered by this Statement is processed and stored in the United States and possibly other jurisdictions and also in other countries where Kaspersky Lab conduct business. All Kaspersky Lab employees are aware of our security policies. Your data is only accessible to those employees who need it in order to perform their jobs. Any stored data will not be associated with any personally identifiable information. Kaspersky Lab does not combine the data stored by Kaspersky Security Network with any data, contact lists, or subscription information that is collected by Kaspersky Lab for promotional or other purposes.

USE OF THE COLLECTED DATA

How Your Personal Information Is Used

Kaspersky Lab collects the data in order to analyze and identify the source of potential security risks, and to improve the ability of Kaspersky Lab's products to detect malicious behavior, fraudulent websites, crimeware, and other types of

Internet security threats to provide the best possible level of protection to Kaspersky Lab customers in the future.

Disclosure of Information to Third Parties

Kaspersky Lab may disclose any of the information collected if asked to do so by a law enforcement official as required or permitted by law or in response to a subpoena or other legal process or if we believe in good faith that we are required to do so in order to comply with applicable law, regulation a subpoena, or other legal process or enforceable government request. Kaspersky Lab may also disclose personally identifiable information when we have reason to believe that disclosing this information is necessary to identify, contact or bring legal action against someone who may be violating this Statement, the terms of your agreements with the Company or to protect the safety of our users and the public or under confidentiality and licensing agreements with certain third parties which assist us in developing, operating and maintaining the Kaspersky Security Network. In order to promote awareness, detection and prevention of Internet security risks, Kaspersky Lab may share certain information with research organizations and other security software vendors. Kaspersky Lab may also make use of statistics derived from the information collected to track and publish reports on security risk trends.

Choices available to you

Participation in Kaspersky Security Network is optional. You can activate and deactivate the Kaspersky Security Network service at any time by visiting the Feedback settings under your Kaspersky Lab product's options page. Please note, however, if you should choose to withhold requested information or data, we may not be able to provide you with some of the services dependent upon the collection of this data.

Once the service period of your Kaspersky Lab product ends, some of the functions of the Kaspersky Lab software may continue to operate, but information will no longer be sent automatically to Kaspersky Lab.

We also reserve the right to send infrequent alert messages to users to inform them of specific changes that may impact their ability to use our services that they have previously signed up for. We also reserve the right to contact you if compelled to do so as part of a legal proceeding or if there has been a violation of any applicable licensing, warranty and purchase agreements.

Kaspersky Lab is retaining these rights because in limited cases we feel that we may need the right to contact you as a matter of law or regarding matters that may be important to you. These rights do not allow us to contact you to market new or existing services if you have asked us not to do so, and issuance of these types of communications is rare.

DATA COLLECTION – RELATED INQUIRIES AND COMPLAINTS

Kaspersky Lab takes and addresses its users' Data Collection concerns with utmost respect and attention. If you believe that there was an instance of non-compliance with this Statement with regard to your information or data you have other related inquiries or concerns, you may write or contact Kaspersky Lab at email: support@kaspersky.com.

In your message, please describe in as much detail as possible the nature of your inquiry. We will investigate your inquiry or complaint promptly.

Provision of information is voluntary. An option of data collection can be disabled by the user at any time in section "**Feedback**" on the page "**Settings**" of any appropriate Kaspersky product.

Copyright © 2008 Kaspersky Lab. All rights reserved.

KASPERSKY LAB

Founded in 1997, Kaspersky Lab has become a recognized leader in information security technologies. It produces a wide range of data security software and delivers high-performance, anti-virus, anti-spam and anti-hacking systems.

Kaspersky Lab is an international company. Headquartered in the Russian Federation, the company has offices in the United Kingdom, France, Germany, Japan, the Benelux countries, China, Poland, Romania and the USA (California). A new company office, the European Anti-Virus Research Centre, has recently been established in France. Kaspersky Lab's partner network includes over 500 companies worldwide.

Today Kaspersky Lab employs over 450 highly qualified specialists including 10 MBA degree holders and 16 PhD degree holders. Senior experts hold membership in the Computer Anti-Virus Researchers Organization (CARO).

The most valuable asset of our company are unique knowledge and expertise accumulated by its specialists during the fourteen years of the never-ceasing fight against computer viruses. A thorough analysis of computer virus activities enables the company's specialists to foresee the malware development trends and delivery to our users a timely protection against new types of attacks. Resistance to future attacks is the basic policy implemented in all Kaspersky Lab's products. At all times, the company's products remain one step ahead of other vendors in delivering anti-virus coverage to our clients.

Years of hard work have made the company one of the top anti-virus software developers. Kaspersky Lab was one of the first businesses of its kind to develop the highest standards for anti-virus defense. The company's flagship product, Kaspersky Anti-Virus, provides full-scale protection for all tiers of a network. workstations, file servers, mail systems, firewalls, internet gateways and hand-held computers. Its convenient and easy-to-use management tools ensure the maximum degree of automation of the anti-virus protection of computers and corporate networks. Many well-known manufacturers use the Kaspersky Anti-Virus kernel. The list of such companies includes Nokia ICG (USA), F-Secure (Finland), Aladdin (Israel), Sybari (USA), G Data (Germany), Deerfield (USA), Alt-N (USA), Microworld (India) and BorderWare (Canada).

Kaspersky Lab's customers benefit from a wide range of additional services that ensure both stable operation of the company's products, and compliance with specific business requirements. We design, implement and support corporate anti-virus complexes. Kaspersky Lab's anti-virus database is updated every hour. The company provides its customers with 24-hour technical support service available in several languages.

IN THIS SECTION:

Other Kaspersky Lab Products 77

Contact Us 86

OTHER KASPERSKY LAB PRODUCTS

Kaspersky Lab's New Agent

Program News Agent is used for quick delivering Kaspersky Lab's news, notification about the "virus weather" and latest events. The application will read the list of available news channels and information contained in them from the Kaspersky Lab's news server at the specified interval.

Additionally, the News Agent allows:

- visualize the "virus weather" in the system panel;
- subscribe or reject the subscription to Kaspersky Lab's news channels;
- receive news on each subscribed channel with the selected frequency; additionally there is a provision for notification about new unread news;
- view news on the subscribed channels;
- view the list of channels and their status;
- open in the browser pages with detailed news.

The News Agent runs under Microsoft Windows and can be used either as a stand-alone application or be included into integrated solutions provided by Kaspersky Lab.

Kaspersky® Online Scanner

This program is a free service available to visitors of the corporate website allowing to perform efficient anti-virus scan of your computer online. Kaspersky OnLine Scanner runs in the browser. This way users can quickly receive

response to their questions related to the infection with malware. In the course of a scan the user can:

- exclude archives and e-mail databases from the scan;
- select standard or extended databases to be used for the scan;
- save results of the scan in txt or html formats.

Kaspersky® OnLine Scanner Pro

This program is a subscription service available to visitors of the corporate website allowing to perform efficient anti-virus scan of your computer and disinfection of infected files online. Kaspersky OnLine Scanner Pro runs directly in the browser. In the course of a scan the user can:

- exclude archives and e-mail databases from the scan;
- select standard or extended databases to be used for the scan;
- disinfect infected objects detected;
- save results of the scan in txt or html formats.

Kaspersky Anti-Virus® Mobile

Kaspersky Anti-Virus Mobile ensures anti-virus protection of mobile devices running Symbian OS and Microsoft Windows Mobile operating systems. The application allows performing a complex anti-virus scan including:

- on-demand scan or the memory of a mobile device, memory cards, individual folders or files. Once an infected object is detected, it will be quarantined or deleted;
- real-time protection: all incoming or modified objects will be scanned as well as files at the attempt to access them;
- protection against sms and mms spam.

Kaspersky Anti-Virus for file servers

The software product ensures reliable protection of file systems of servers running under Microsoft Windows, Novell NetWare and Linux operating systems against all types of malware. The structure of this software product includes the following Kaspersky Lab's applications:

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Windows Server.

- Kaspersky Anti-Virus for Linux File Server.
- Kaspersky Anti-Virus for Novell Netware.
- Kaspersky Anti-Virus for Samba Server.

Advantages and functional capabilities:

- *real-time protection of the servers' file systems:* all servers' files will be scanned at the attempt to open or save them to the server.
- *preventing virus outbreaks;*
- *on-demand scan* of the entire file system or its individual folders and files;
- *the use of the optimization technologies* when scanning objects of the server's file system;
- *restoring the system after the infection*;
- *scalability of the software product* to match the available system resources;
- *maintaining the system load balance;*
- *creation of the list of trusted processes*, whose activities on the server will not be monitored by this product;
- *remote management* of the product, including centralized installation, configuration and management;
- *storing backup copies of infected and deleted objects* in case their restoration is required;
- *isolation of suspicious* objects in the special storage;
- *notification about events* occurring during the operation of the product sent to the system administrator;
- *maintaining detailed reports;*
- *automatic updating* of the databases of the software product.

Kaspersky Open Space Security

Kaspersky Open Space Security is a software product implementing a new approach to the security of modern corporate networks of any scale and ensuring centralized protection of information systems and support of remote offices and mobile users.

This software product includes four programs:

- Kaspersky Open Space Security.
- Kaspersky Business Space Security.
- Kaspersky Enterprise Space Security.
- Kaspersky Total Space Security.

Provided below is the detailed description of each product.

Kaspersky Work Space Security is a product designed to provide centralized protection of workstations in the corporate network and beyond it against all types of modern internet threats: viruses, spyware, hacking attacks and spam.

Advantages and functional capabilities:

- *comprehensive protection against viruses, hacking attacks and spam;*
- *proactive protection against new malware programs records about which have not been yet added to the databases;*
- *personal firewall with the system for detection of intrusions an prevention of network attacks;*
- *rollback of malicious changes made to the system;*
- *protection against phishing attacks and spam;*
- *dynamic reallocation of resources during the full system scan;*
- *remote management of the product, including centralized installation, configuration and management;*
- *support of Cisco® NAC (Network Admission Control);*
- *scan of e-mail and internet traffic in the real-time mode;*
- *blocking pop-up windows and advertising banners in the Internet;*
- *secure work in networks of any type including Wi-Fi;*
- *tools for creation of rescue disks allowing restoration after a virus attack;*
- *developed system of reports about the protection status;*

- *automatic database updating;*
- *full-fledged support of 64-bit operating systems;*
- *optimization of the laptop software (Intel® Centrino® Duo technology for mobile PC);*
- *ability to perform remote disinfection (Intel® Active Management technology, component Intel® vPro™).*

Kaspersky Business Space Security ensures optimal protection of information resources against modern internet threats. Kaspersky Business Space Security protects workstations and file servers against all types of viruses, Trojan programs and worms preventing virus outbreaks and ensures security of the information as well as the instant access to network resources for users.

Advantages and functional capabilities:

- *remote management of the product, including centralized installation, configuration and management;*
- *support of Cisco® NAC (Network Admission Control);*
- *protection of workstations and file servers against all types of internet threats;*
- *the use of iSwift technology to rule out repetitive scans within the network;*
- *distribution of load between the server's processors;*
- *isolation of suspicious objects in the special storage;*
- *rollback of malicious changes made to the system;*
- *scalability of the software product to match the available system resources;*
- *proactive protection of workstations against new malware programs records about which have not been yet added to the databases;*
- *scan of e-mail and internet traffic in the real-time mode;*
- *personal firewall with the system for detection of intrusions an prevention of network attacks;*
- *protection of operation within Wi-Fi wireless networks;*
- *self-protection technology of the anti-virus against malware;*

- *isolation of suspicious objects in the special storage;*
- *automatic database updating.*

Kaspersky Enterprise Space Security

This software product includes components for protection of workstations and teamwork servers against all types of modern internet threats, removes viruses from the e-mail streams, ensures security of information and instant users' access to the network resources.

Advantages and functional capabilities:

- *protection of workstations and servers against viruses, Trojan programs and worms;*
- *protection of mail servers Sendmail, Qmail, Postfix and Exim;*
- *scan of all messages on the Microsoft Exchange server including shared folders;*
- *processing messages, databases and other objects of Lotus Domino servers;*
- *protection against phishing attacks and spam;*
- *preventing mass mailings and virus outbreaks;*
- *scalability of the software product to match the available system resources;*
- *remote management of the product, including centralized installation, configuration and management;*
- *support of Cisco® NAC (Network Admission Control);*
- *proactive protection of workstations against new malware programs records about which have not been yet added to the databases;*
- *personal firewall with the system for detection of intrusions an prevention of network attacks;*
- *secure work within Wi-Fi wireless networks;*
- *scan of internet traffic in the real-time mode;*
- *rollback of malicious changes made to the system;*
- *dynamic reallocation of resources during the full system scan;*

- *isolation of suspicious objects in the special storage;*
- *developed system of reports about the protection system status;*
- *automatic database updating.*

Kaspersky Total Space Security

This solution controls all incoming and outgoing data streams - e-mail, web traffic and all network interactions. The product includes components used to protect workstations and mobile devices, ensures instant and secure user access to the corporate information resources and Internet and guarantees secure communication by e-mail.

Advantages and functional capabilities:

- *comprehensive protection against viruses, hacking attacks and spam at all levels of the corporate network; from workstations to gateways;*
- *proactive protection of workstations against new malware programs records about which have not been yet added to the databases;*
- *protection of mail servers and shared servers;*
- *real-time scan of incoming LAN web traffic (HTTP / FTP);*
- *scalability of the software product to match the available system resources;*
- *blocking access from infected workstations;*
- *preventing virus outbreaks;*
- *centralized reports about the protection status;*
- *remote management of the product, including centralized installation, configuration and management;*
- *support of Cisco® NAC (Network Admission Control);*
- *support of hardware proxy servers;*
- *filtering internet traffic according to the list of trusted servers, types of objects and groups of users;*
- *the use of iSwift technology to rule out repetitive scans within the network;*

- *dynamic reallocation of resources during the full system scan;*
- *personal firewall with the system for detection of intrusions an prevention of network attacks;*
- secure work in networks of any type including Wi-Fi;
- *protection against phishing attacks and spam;*
- *ability to perform remote disinfection (Intel® Active Management technology, component Intel® vPro™);*
- *rollback of malicious changes made to the system;*
- *self-protection technology of the anti-virus against malware;*
- *full-fledged support of 64-bit operating systems;*
- automatic database updating.

Kaspersky Security for Mail Servers

Software product for protection of mail servers and shared servers against malware programs and spam. The product includes applications for protection of all popular mail servers: Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix and Exim and allows arranging a dedicated mail gateway. This solution includes:

- Kaspersky Administration Kit.
- Kaspersky Mail Gateway.
- Kaspersky Anti-Virus for Lotus Notes/Domino.
- Kaspersky Anti-Virus for Microsoft Exchange.
- Kaspersky Anti-Virus® for Linux Mail Server

The capabilities of this program include:

- *reliable protection against malware and potentially dangerous programs;*
- *filtering spam;*
- *scan of incoming and outgoing mail messages and attachments;*
- *anti-virus scan of all messages on the Microsoft Exchange* server including shared folders;

- *scan of messages, databases and other objects of Lotus Domino servers;*
- *filtering messages* by attachments types;
- *isolation of suspicious* objects in the special storage;
- *convenient system for managing* the software product;
- *preventing virus outbreaks;*
- *monitoring of the protection system status* using notifications;
- *system of reports* about operation of the application;
- *scalability of the software product* to match the available system resources;
- *automatic database updating.*

Kaspersky Security for Gateways

This software product ensures the secure access to the Internet for all employees of the company automatically removing malware and riskware from the flow of data received by the network via HTTP/FTP protocols. This solution includes:

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Proxy Server.
- Kaspersky Anti-Virus for Microsoft ISA Server.
- Kaspersky Anti-Virus for Check Point FireWall-1.

The capabilities of this program include:

- *reliable protection against malware and potentially dangerous programs;*
- *scan of internet traffic* (HTTP/FTP) in the real-time mode;
- *filtering internet traffic* according to the list of trusted servers, types of objects and groups of users;
- *isolation of suspicious* objects in the special storage;
- *convenient control system;*
- *system of reports about operation of the application;*

- *support of hardware proxy servers;*
- *scalability of the software product* to match the available system resources;
- *automatic database updating.*

Kaspersky® Anti-Spam

Kaspersky Anti-Spam is the first Russian software package used to ensure protection against spam for small and medium-size companies. This product combines revolutionary technologies of the linguistic analysis of texts, all modern methods of filtering e-mail (including DNS Back List and formal attributes of messages) and a unique set of services which allow the user to detect and eliminate up to 95 percent of unwanted traffic.

Kaspersky Anti-Spam is a filter set at the "entrance" of the corporate network scanning the incoming flow of messages for spam. It is compatible with any mail system used in the client's network and can be installed on the existing mail server or on a dedicated server.

High efficiency of the program is achieved due to the daily automatic update of the content filtering databases with samples provided by the specialists of linguistic lab. Updates are released every 20 minutes.

Kaspersky Anti-Virus® for MIMESweeper

Kaspersky Anti-Virus ® for MIMESweeper ensures high-speed anti-virus traffic scan for servers using Clearswift MIMEsweeper for SMTP / Clearswift MIMEsweeper for Exchange / Clearswift MIMEsweeper for Web.

The application is implemented as a plug-in (extension module) and performs a real-time anti-virus scan and processing of incoming and outgoing e-mail messages.

CONTACT US

If you have any quetions, you can contact our dealers or contact Kaspersky Lab directly. Detailed consultations are provided by phone or e-mail. You will receive full and comprehensive answers to any question.

Address:	Russia, 123060, Moscow, 1-st Volokolamsky Proezd, 10, Building 1

Tel., Fax:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00
24/7 Emergency Support	+7 (495) 797-87-07, +7 (495) 645-79-29, +7 (495) 956-87-08
Support of business product users:	+7 (495) 797-87-07, +7 (495) 645-79-29, +7 (495) 956-87-08 (from 10 am until 7 pm) http://support.kaspersky.com/helpdesk.html
Support for corporate users:	contact information will be provided after you purchase a corporate software product depending on your support package.
Kaspersky Lab web forum:	http://forum.kaspersky.com
Anti-Virus Lab:	newvirus@kaspersky.com (only for sending new viruses in archives)
User documentation development group	docfeedback@kaspersky.com (only for sending feedback on documentation and Help system)
Sales Department:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00 sales@kaspersky.com
General Information:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00 info@kaspersky.com
WWW:	http://www.kaspersky.com http://www.viruslist.com

CRYPTOEX LLC

For creation and verification of the digital signature Kaspersky Anti-Virus uses data security software library Crypto C developed by Crypto Ex LLC.

Crypto Ex is a holder of Federal Agency for Government Communications and Information (FSB - Federal Security Service) license for development, manufacture and distribution of encrypting complex systems for ensuring security of data not constituting a state secret.

Library Crypto C is designed for the use in the systems for complex protection of KS1 class confidential information and is granted FSB compliance certificate No. SF/114-0901 dated July 1, 2006.

Modules of this library use encryption and decryption of fixed size data packs and/or data flows based on the use of a cryptographic algorithm (GOST 28147-89), generation and verification of electronic digital signature based on algorithms (GOST R 34.10-94 and GOST 34.10-2001), hash function (GOST 34.11-94), generation of key information using a pseudorandom number program transmitter. Additionally, CryptoEx LLC implemented a key information and simulation vector generation system (GOST 28147-89).

Library modules were implemented using C programming language (in accordance with ANSI C standard) and can be integrated into applications as statically and dynamically loaded code and can be executed on platforms x86, x86-64, Ultra SPARC II as well as compatible platforms.

Library modules can be migrated to the following operating environments: Microsoft Windows NT/XP/98/2000/2003, Unix (Linux, FreeBSD, SCO Open Unix 8.0, SUN Solaris, SUN Solaris for Ultra SPARC II).

CryptoEx LLC corporate website: http://www.cryptoex.ru

E-mail: info@cryptoex.ru

MOZILLA FOUNDATION

Library **Gecko SDK ver. 1.8** was used for the development of the application's component.

This software is used according to the terms and conditions of license MPL 1.1 Public Mozilla Foundation license http://www.mozilla.org/MPL.

For more details about this library Gecko SDK refer to: http://developer.mozilla.org/en/docs/Gecko_SDK.

© Mozilla Foundation

Mozilla Foundation website: http://www.mozilla.org.

LICENSE AGREEMENT

Standard End User License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT"), FOR THE LICENSE OF KASPERSKY INTERNET SECURITY ("SOFTWARE") PRODUCED BY KASPERSKY LAB ("KASPERSKY LAB").

IF YOU HAVE PURCHASED THIS SOFTWARE VIA THE INTERNET BY CLICKING THE ACCEPT BUTTON, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) CONSENT TO BE BOUND BY AND BECOME A PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT AND DO NOT INSTALL THE SOFTWARE.

IF YOU HAVE PURCHASED THIS SOFTWARE ON A PHYSICAL MEDIUM, HAVING BROKEN THE CD'S SLEEVE YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT DO NOT BREAK THE CD's SLEEVE, DOWNLOAD, INSTALL OR USE THIS SOFTWARE.

IN ACCORDANCE WITH THE LEGISLATION, REGARDING KASPERSKY SOFTWARE INTENDED FOR INDIVIDUAL CONSUMERS AND PURCHASED ONLINE FROM THE KASPERSKY LAB OR ITS PARTNER'S INTERNET WEB SITE, CUSTOMER SHALL HAVE A PERIOD OF FOURTEEN (14) WORKING DAYS AS FROM THE DELIVERY OF PRODUCT TO MAKE RETURN OF IT TO THE MERCHANT FOR EXCHANGE OR REFUND, PROVIDED THE SOFTWARE IS NOT UNSEALED.

REGARDING THE KASPERSKY SOFTWARE INTENDED FOR INDIVIDUAL CONSUMERS NOT PURCHASED ONLINE VIA INTERNET, THIS SOFTWARE NEITHER WILL BE RETURNED NOR EXCHANGED EXCEPT FOR CONTRARY PROVISIONS FROM THE PARTNER WHO SELLS THE PRODUCT. IN THIS CASE, KASPERSKY LAB WILL NOT BE HELD BY THE PARTNER'S CLAUSES.

THE RIGHT TO RETURN AND REFUND EXTENDS ONLY TO THE ORIGINAL PURCHASER.

All references to "Software" herein shall be deemed to include the software activation code with which you will be provided by Kaspersky Lab as a part of the Kaspersky Internet Security 2009.

1. *License Grant*. Subject to the payment of the applicable license fees, and subject to the terms and conditions of this Agreement, Kaspersky Lab hereby grants you the non-exclusive, non-transferable right to use one copy of the specified version of the Software and the accompanying documentation (the "Documentation") for the term of this Agreement solely for your own internal business purposes. You may install one copy of the Software on one computer.

1.1 *Use*. The Software is licensed as a single product; it may not be used on more than one computer or by more than one user at a time, except as set forth in this Section.

1.1.1 The Software is "in use" on a computer when it is loaded into the temporary memory (i.e., random-access memory or RAM) or installed into the permanent memory (e.g., hard disk, CD-ROM, or other storage device) of that computer. This license authorizes you to make only as many back-up copies of the Software as are necessary for its lawful use and solely for back-up purposes, provided that all such copies contain all of the Software's proprietary notices. You shall maintain records of the number and location of all copies of the Software and Documentation and will take all reasonable precautions to protect the Software from unauthorized copying or use.

1.1.2 The Software protects computer against viruses and network attacks whose signatures are contained in the threat signatures and network attacks databases which are available on Kaspersky Lab's update servers.

1.1.3 If you sell the computer on which the Software is installed, you will ensure that all copies of the Software have been previously deleted.

1.1.4 You shall not decompile, reverse engineer, disassemble or otherwise reduce any part of this Software to a humanly readable form nor permit any third party to do so. The interface information necessary to achieve interoperability of the Software with independently created computer programs will be provided by Kaspersky Lab by request on payment of its reasonable costs and expenses for procuring and supplying such information. In the event that Kaspersky Lab notifies you that it does not intend to make such information available for any reason, including (without limitation) costs, you shall be permitted to take such steps to achieve interoperability, provided that you only reverse engineer or decompile the Software to the extent permitted by law.

1.1.5 You shall not make error corrections to, or otherwise modify, adapt, or translate the Software, nor create derivative works of the Software, nor permit any third party to copy (other than as expressly permitted herein).

1.1.6 You shall not rent, lease or lend the Software to any other person, nor transfer or sub-license your license rights to any other person.

1.1.7 You shall not provide the activation code or license key file to third parties or allow third parties access to the activation code or license key. The activation code and license key are confidential data.

1.1.8 Kaspersky Lab may ask User to install the latest version of the Software (the latest version and the latest maintenance pack).

1.1.9 You shall not use this Software in automatic, semi-automatic or manual tools designed to create virus signatures, virus detection routines, any other data or code for detecting malicious code or data.

1.1.10 You have the right to provide to Kaspersky Lab information about potential threats and vulnerabilities from your computer, more details specified in Data Collection statement. The information gathered is used in a general form for the purpose of improving Kaspersky Lab's products only.

1.1.11 For the purposes stated in clause 1.1.10 Software will automatically collect information about checksums of files, executed on a computer, and send them to Kaspersky Lab.

Support[1].

(i) Kaspersky Lab will provide you with the support services ("Support Services") as defined below for a period, specified in the License Key File and indicated in the "Service" window, since the moment of activation on:

(a) payment of its then current support charge, and:

(b) successful completion of the Support Services Subscription Form as provided to you with this Agreement or as available on the Kaspersky Lab website, which will require you to enter activation code also provided to you by Kaspersky Lab with this Agreement. It shall be at the absolute discretion of Kaspersky Lab whether or not

[1] When using demo software, you are not entitled to the Technical Support specified in Clause 2 of this EULA, nor do you have the right to sell the copy in your possession to other parties.

You are entitled to use the software for demo purposes for the period of time specified in the license key file starting from the moment of activation (this period can be viewed in the Service window of the software's GUI).

you have satisfied this condition for the provision of Support Services.

Support Services shall become available after Software activation. Kaspersky Lab's technical support service is also entitled to demand from you additional registration for identifier awarding for Support Services rendering.

Until Software activation and/or obtaining of the End User identifier (Customer ID) technical support service renders only assistance in Software activation and registration of the End User.

(ii) Support Services will terminate unless renewed annually by payment of the then-current annual support charge and by successful completion of the Support Services Subscription Form again.

(iii) "Support Services" means:

(a) Regular updates of the anti-virus database;

(b) Updates of network attacks database;

(c) Updates of anti-spam database;

(d) Free software updates, including version upgrades;

(e) Technical support via Internet and hot phone-line provided by Vendor and/or Reseller;

(f) Virus detection and disinfection updates in 24-hours period.

(iv) Support Services are provided only if and when you have the latest version of the Software (including maintenance packs) as available on the official Kaspersky Lab website (www.kaspersky.com) installed on your computer.

3. *Ownership Rights*. The Software is protected by copyright laws. Kaspersky Lab and its suppliers own and retain all rights, titles and interests in and to the Software, including all copyrights, patents, trademarks and other intellectual property rights therein. Your possession, installation, or use of the Software does not transfer any title to the intellectual property in the Software to you, and you will not acquire any rights to the Software except as expressly set forth in this Agreement.

4. *Confidentiality*. You agree that the Software and the Documentation, including the specific design and structure of individual programs constitute confidential proprietary information of Kaspersky Lab. You shall not disclose, provide, or

otherwise make available such confidential information in any form to any third party without the prior written consent of Kaspersky Lab. You shall implement reasonable security measures to protect such confidential information, but without limitation to the foregoing shall use best endeavours to maintain the security of the activation code.

5. *Limited Warranty*.

(i) Kaspersky Lab warrants that for six (6) months from first download or installation the Software purchased on a physical medium will perform substantially in accordance with the functionality described in the Documentation when operated properly and in the manner specified in the Documentation.

(ii) You accept all responsibility for the selection of this Software to meet your requirements. Kaspersky Lab does not warrant that the Software and/or the Documentation will be suitable for such requirements nor that any use will be uninterrupted or error free.

(iii) Kaspersky Lab does not warrant that this Software identifies all known viruses and spam letters, nor that the Software will not occasionally erroneously report a virus in a title not infected by that virus.

(iv) Your sole remedy and the entire liability of Kaspersky Lab for breach of the warranty at paragraph (i) will be at Kaspersky Lab option, to repair, replace or refund of the Software if reported to Kaspersky Lab or its designee during the warranty period. You shall provide all information as may be reasonably necessary to assist the Supplier in resolving the defective item.

(v) The warranty in (i) shall not apply if you (a) make or cause to be made any modifications to this Software without the consent of Kaspersky Lab, (b) use the Software in a manner for which it was not intended, or (c) use the Software other than as permitted under this Agreement.

(vi) The warranties and conditions stated in this Agreement are in lieu of all other conditions, warranties or other terms concerning the supply or purported supply of, failure to supply or delay in supplying the Software or the Documentation which might but for this paragraph (vi) have effect between Kaspersky Lab and your or would otherwise be implied into or incorporated into this Agreement or any collateral contract, whether by statute, common law or *otherwise*, all of which are hereby excluded (including, without limitation, the implied conditions, warranties or other terms as to satisfactory quality, fitness for purpose or as to the use of reasonable skill and care).

6. *Limitation of Liability*.

(i) Nothing in this Agreement shall exclude or limit Kaspersky Lab's liability for (a) the tort of deceit, (b) death or personal injury caused by its

breach of a common law duty of care or any negligent breach of a term of this Agreement, or (c) any other liability which cannot be excluded by law.

(ii) Subject to paragraph (i) above, Kaspersky Lab shall bear no liability (whether in contract, tort, restitution or otherwise) for any of the following losses or damage (whether such losses or damage were foreseen, foreseeable, known or otherwise):

(a) Loss of revenue;

(b) Loss of actual or anticipated profits (including for loss of profits on contracts);

(c) Loss of the use of money;

(d) Loss of anticipated savings;

(e) Loss of business;

(f) Loss of opportunity;

(g) Loss of goodwill;

(h) Loss of reputation;

(i) Loss of, damage to or corruption of data, or:

(j) Any indirect or consequential loss or damage howsoever caused (including, for the avoidance of doubt, where such loss or damage is of the type specified in paragraphs (ii), (a) to (ii), (i).

(iii) Subject to paragraph (i) above, the liability of Kaspersky Lab (whether in contract, tort, restitution or otherwise) arising out of or in connection with the supply of the Software shall in no circumstances exceed a sum equal to the amount equally paid by you for the Software.

7. This Agreement contains the entire understanding between the parties with respect to the subject matter hereof and supersedes all and any prior understandings, undertakings and promises between you and Kaspersky Lab, whether oral or in writing, which have been given or may be implied from anything written or said in negotiations between us or our representatives prior to this Agreement and all prior agreements between the parties relating to the matters aforesaid shall cease to have effect as from the Effective Date.